Sicherheitsschichten im Eisenbahnsystem

Von der Fakultät für Maschinenbau
der Technischen Universität Carolo-Wilhelmina zu Braunschweig

zur Erlangung der Würde

einer Doktor-Ingenieurin (Dr.-Ing.)

genehmigte Dissertation

von:	Dipl.-Math. Stefanie Schwartz
aus (Geburtsort):	Hamburg

eingereicht am:	12. Januar 2012
mündliche Prüfung am:	15. Juni 2012
Referenten:	Prof. Dr.-Ing. Karsten Lemmer Prof. Dr.-Ing. Dr. h. c. mult. Eckehard Schnieder

2012

Berichte aus dem DLR-Institut für Verkehrssystemtechnik

Band 20

Sicherheitsschichten im Eisenbahnsystem

Stefanie Schwartz

Herausgeber:
Deutsches Zentrum für Luft- und Raumfahrt e. V.
Institut für Verkehrssystemtechnik
Lilienthalplatz 7, 38108 Braunschweig

ISSN: 1866-721X

DLR-TS 1.20

Braunschweig, im Dezember 2012

Institutsdirektor:
Prof. Dr.-Ing. Karsten Lemmer

Verfasserin:
Stefanie Schwartz

Vorwort des Herausgebers

Liebe Leserinnen und Leser,

In Ihren Händen halten Sie einen Band unserer Buchreihe „Berichte aus dem DLR-Institut für Verkehrssystemtechnik“. In dieser Reihe veröffentlichen wir spannende, wissenschaftliche Themen aus dem Institut für Verkehrssystemtechnik des Deutschen Zentrums für Luft- und Raumfahrt e. V. (DLR) und aus seinem Umfeld. Einen Teil der Auflage stellen wir Bibliotheken und Fachbibliotheken für ihren Buchbestand zur Verfügung. Herausragende wissenschaftliche Arbeiten und Dissertationen finden hier ebenso Platz wie Projektberichte und Beiträge zu Tagungen in unserem Hause von verschiedenen Referenten aus Wirtschaft, Wissenschaft und Politik.

Mit dieser Veröffentlichungsreihe verfolgen wir das Ziel, einen weiteren Zugang zu wissenschaftlichen Arbeiten und Ergebnissen zu ermöglichen. Wir nutzen die Reihe auch als praktische Nachwuchsförderung durch die Publikation der wissenschaftlichen Ergebnisse von Dissertationen unserer Mitarbeiter und auch externer Doktoranden. Veröffentlichungen sind wichtige Meilensteine auf dem akademischen Berufsweg. Mit der Reihe „Berichte aus dem DLR-Institut für Verkehrssystemtechnik“ erweitern wir das Spektrum der möglichen Publikationen um einen Baustein. Darüber hinaus verstehen wir die Kommunikation unserer Forschungsthemen als Beitrag zur nationalen und internationalen Forschungslandschaft auf den Gebieten Automotive, Bahnsysteme und Verkehrsmanagement.

Die vorliegende Dissertation unserer Buchreihe beschäftigt sich mit einem hochaktuellen und überaus wichtigen Thema: Sicherheit im Schienenverkehr. Bevor sicherheitsrelevante Eisenbahnanlagen oder -fahrzeuge nach Änderungen oder Neubau in Betrieb genommen werden dürfen, muss das Eisenbahnunternehmen die Sicherheit dieser Systeme nachweisen. Eine der größten Herausforderungen dabei ist die Unterscheidung zwischen sicherheitsrelevanten und nicht-sicherheitsrelevanten Systemelementen. Die vorliegende Arbeit entwickelt am Beispiel eines Bahnübergangs eine neue erfolgversprechende Methode zur *I*dentifikation von sogenannten *S*icherheitsschichten im *E*isenbahn*s*ystem: die ISES-Methode. Sie findet ihre Anwendung aber nicht nur im Eisenbahnbereich, sondern lässt sich auch auf andere Domänen übertragen, in denen hohe Sicherheitsanforderungen berücksichtigt werden müssen. Damit leistet diese Dissertation nicht nur einen wertvollen Beitrag für den Schienenverkehr der Zukunft, sondern bietet darüber hinaus mit der ISES-Methode auch eine geeignete Ebene für domänenübergreifenden fachlichen Austausch von Sicherheitsexperten. So können verschiedene Sicherheitskonzepte verglichen und Synergien genutzt werden.

Prof. Dr.-Ing. Karsten Lemmer

Vorwort der Autorin

Die vorliegende Arbeit entstand auf Basis meiner Tätigkeiten als wissenschaftliche Mitarbeiterin am Institut für Verkehrssystemtechnik des Deutschen Zentrums für Luft- und Raumfahrt e. V. (DLR) in Braunschweig.

Dem Institutsleiter, Herrn Prof. Dr.-Ing. Karsten Lemmer, als meinem Doktorvater, danke ich für die langjährige Begleitung und Unterstützung meiner Arbeit. Die Forschungstätigkeiten am Institut haben mir das Thema Sicherheit im Eisenbahnbereich erschlossen.

Herrn Prof. Dr.-Ing. Dr. h. c. mult. Eckehard Schnieder, Leiter des Instituts für Verkehrssicherheit und Automatisierungstechnik an der TU Braunschweig, danke ich für sein Interesse an meiner Arbeit und für die Übernahme des Korreferats.

Herrn Prof. Dr.-Ing. Thomas Vietor, Leiter des Instituts für Konstruktionstechnik an der TU Braunschweig, danke ich für die Übernahme des Vorsitzes der Prüfungskommission.

Ebenfalls bedanken möchte ich mich bei meinen Kollegen am DLR für die angenehme Atmosphäre, die gute Teamarbeit und die interessanten Forschungsthemen. Mein besonderer Dank gilt Herrn Dr.-Ing. Michael Meyer zu Hörste, der mir während meiner Zeit am Institut stets Herausforderungen gestellt hat, an denen ich wachsen konnte. Die regen fachlichen Diskussionen methodischer Ideen haben viel zum Gelingen meiner Dissertation beigetragen. Bei Herrn Dr.-Ing. Markus Pelz bedanke ich mich für die guten Ideen, die den Grundstein zu dieser Arbeit gelegt haben.

Meinen Kollegen beim TÜV SÜD danke ich für die thematischen Anregungen und Kommentare und für die Freiräume, die es mir ermöglicht haben diese Arbeit fertigstellen zu können.

Dankbar bin ich für den Rückhalt meiner Familie, für das Vertrauen und die Hilfe, die mir das Studium ermöglicht hat und ohne die diese Dissertation nicht möglich gewesen wäre. Mein ganz besonderer Dank gilt meiner Mutter, die mich stets unterstützt und ermutigt hat, immer noch einen Schritt weiterzugehen. Bei meinem Lebensgefährten Rainer bedanke ich mich für das Verständnis und die stetige Unterstützung. Marlies danke ich für den ganz anderen Blickwinkel.

Dipl.-Math. Stefanie Schwartz

Diese Dissertation widme ich
meiner viel zu früh verstorbenen Mutter
Felicitas Schwartz.

Inhaltsverzeichnis

Vorwort des Herausgebers iii

Vorwort der Autorin v

Kurzfassung xi

Abstract xiii

1 Einleitung 1
- 1.1 Motivation . . . 1
- 1.2 Ziel . . . 3
- 1.3 Struktur der vorliegenden Arbeit . . . 4

2 Verbreitete Begriffe und Konzepte 7
- 2.1 Normen . . . 7
- 2.2 Basisbegriffe . . . 8
- 2.3 Begriffe aus dem Umfeld der Sicherheitsschichten . . . 10

3 Sicherheitsschichten 17
- 3.1 Anforderungen an Sicherheitsschichten . . . 17
- 3.2 Definition des Begriffs Sicherheitsschicht . . . 18
- 3.3 Vergleich mit anderen Definitionen . . . 23
- 3.4 Eigenschaften von Sicherheitsschichten . . . 25
- 3.5 Verwendbarkeit von Sicherheitsschichten . . . 26

4 Modelle und Darstellungsweisen 29
- 4.1 Anforderungen an die Darstellungsweise . . . 29
- 4.2 Energiemodell . . . 30
- 4.3 Zwiebelschalenmodell . . . 31
- 4.4 Layer-of-Protection-Analysis-Diagramm (LOPA-Diagramm) . . . 32
- 4.5 Dominomodell . . . 33
- 4.6 Schweizer-Käse-Modell (Swiss Cheese Model) . . . 35
- 4.7 Fliegendiagramm (Bow-Tie Diagram) . . . 36
- 4.8 Event and Barrier Function Model . . . 37
- 4.9 Accident Evolution and Barrier function model . . . 37
- 4.10 Sicherheitsbarrierendiagramm . . . 38
- 4.11 Barriereblockdiagramm . . . 39
- 4.12 Vergleich der Darstellungsweisen . . . 40

5 Vorhandene Methoden 43
- 5.1 Anforderungen an die gesuchte Methode . . . 44
- 5.2 Methoden im Überblick . . . 44
- 5.3 Why-Because-Analyse . . . 46
- 5.4 Sicherheitsfunktionsanalyse . . . 48

5.5 Barriereanalyse . . . 49
5.6 Fehlerbaumanalyse . . . 51
5.7 Ereignisbaumanalyse . . . 53
5.8 Accident Evolution and Barrier function Methode . . . 55
5.9 Schutzebenenanalyse . . . 56
5.10 Vergleich der Methoden . . . 57

6 ISES-Methode 61
6.1 Gesamtrahmen der Methode zur Identifikation von Sicherheitsschichten . . . 61
6.2 Voraussetzungen für die Anwendung der ISES-Methode . . . 62
6.3 Schritt A: Fehlerbaumanalyse für das System . . . 63
6.4 Schritt B: Identifikation von Barrieren mit Hilfe der Fehlerbaumanalyse . . . 67
6.5 Schritt C: Identifikation von Barriere-Funktions-Paaren mit Hilfe von Checklisten . . . 73
6.6 Schritt D: Prüfen auf Wirksamkeit und Unabhängigkeit . . . 80

7 Regeln und Anwendungshinweise 87
7.1 Zeitpunkt der Anwendung der ISES-Methode . . . 87
7.2 Darstellung von Sicherheitsschichten . . . 87
7.3 Modell und Methode bei mehreren Gefährdungen . . . 91
7.4 Über das Glück . . . 92
7.5 Methoden zur Bewertung von Sicherheitsschichten . . . 92
7.6 Vorgehen zum Austausch von Sicherheitsschichten . . . 94

8 Anwendungsbeispiel: Bahnübergang 97
8.1 Arten von Bahnübergängen . . . 98
8.2 Beschreibung eines Bahnübergangs mit Überwachungssignal . . . 100
8.3 Zu untersuchende Gefährdung . . . 101

9 Anwendung der ISES-Methode auf den Beispiel-Bahnübergang 103
9.1 Schritt A: Fehlerbaumanalyse . . . 103
9.2 Schritt B: Identifikation von Barrieren mit Hilfe der Fehlerbaumanalyse . . . 104
9.3 Schritt C: Identifikation von Barriere-Funktions-Paaren mit Hilfe von Checklisten . . . 105
9.4 Schritt D: Prüfen auf Wirksamkeit und Unabhängigkeit . . . 121
9.5 Veränderung des Beispiel-Bahnübergangs durch die Einführung von ETCS . . . 124

10 Validierung und weiterführende Betrachtungen 129
10.1 Erfüllung der Anforderungen an Sicherheitsschichten und an die ISES-Methode . . . 129
10.2 Verbindung zwischen Sicherheitsschichten und Unfallanalysen . . . 138

11 Zusammenfassung und Ausblick 145
11.1 Zusammenfassung . . . 145
11.2 Ausblick . . . 146

Anhang 149

A Fehlerbaum 149

B Checkliste 151

C Bahnübergang Wupperweg 157
C.1 Artikel 1 . . . 157
C.2 Artikel 2 . . . 158

C.3 Artikel 3 159
C.4 Artikel 4 160
C.5 Weitere Informationen 161

Glossar **167**

Abkürzungen **171**

Literaturverzeichnis **175**

Index **183**

Kurzfassung

Bei der Entwicklung von neuen und der Änderung von bereits bestehenden Eisenbahnsystemen ist die Sicherheit ein elementarer Aspekt. Neue Systeme müssen in Deutschland den anerkannten Regeln der Technik entsprechen oder mindestens die gleiche Sicherheit wie bei der Beachtung dieser Regeln aufweisen. Änderungen an einem bestehenden System dürfen nicht zu einer Verschlechterung der Sicherheit führen. Durch die neue europäische Gesetzgebung kann die ausreichende Sicherheit eines Systems auch durch den Vergleich mit einem Referenzsystem bestimmt werden.
Die Frage nach der ausreichenden Sicherheit von neuen oder geänderten Eisenbahnsystemen wird demnach durch einen Vergleich beantwortet. Um diesen Vergleich nach den anerkannten Regeln der Technik oder mit einem anderen System durchführen zu können, müssen die sicherheitsrelevanten Teile des Systems identifiziert werden. Die Unterscheidung zwischen sicherheitsrelevanten und nicht-sicherheitsrelevanten Systemelementen und Regeln fällt jedoch vielen Fachleuten schwer. Eine Ursache hierfür ist die in der Regel für die Sicherheitsanalyse ungeeignete Darstellung von Systemdokumentation und Regelwerken. Sie erschwert die Analyse, aber auch die Bewertung, Begutachtung und Zulassung des Systems.
Ziel der vorliegenden Arbeit ist es, den an der Sicherheitsanalyse und -bewertung beteiligten Fachleuten ein Hilfsmittel zur Verfügung zu stellen, das diesen Vergleich erleichtert.
Dazu wird zunächst der neue Begriff Sicherheitsschicht eingeführt und klar definiert. Die Sicherheitsschichten eines Systems bilden die Elemente für einen Vergleich der Sicherheit zweier Systeme. Um eine Unterscheidung zwischen allgemeinen Sicherheitsmaßnahmen und Sicherheitsschichten zu ermöglichen, wird ein Katalog von Kriterien ausgearbeitet, mit dessen Hilfe geprüft wird, ob es sich bei einer Sicherheitsmaßnahme um eine Sicherheitsschicht handelt.
Um die systematische Identifikation von Sicherheitsschichten in einem Eisenbahnsystem zu ermöglichen, wird im Rahmen der vorliegenden Arbeit eine neue Methode entwickelt: die Methode zur Identifikation von Sicherheitsschichten in Eisenbahnsystemen (ISES-Methode). Diese neue Methode ist so gestaltet, dass sie sich in den bestehenden Ablauf bei der Sicherheitsanalyse und -nachweisführung einfügt.
Die Anwendung der ISES-Methode und der Nutzen der Identifikation von Sicherheitsschichten werden am Beispiel eines Bahnübergangs demonstriert. Im Rahmen einer Validierung wird geprüft, ob die Anforderungen für einen bestimmungsgemäßen Gebrauch des Begriffs Sicherheitsschicht und der ISES-Methode erfüllt werden. Durch eine weiterführende Betrachtung der Schnittstelle zwischen den Ergebnissen der ISES-Methode und Unfallanalysen wird der Kreis der Sicherheitsbetrachtung geschlossen.

Abstract

When developing new railway systems or changing existing ones, safety is a fundamental aspect. In Germany, new systems have to be built according to codes of practice. If they are not, they must have at least the same safety as if the codes of practice would have been applied. Changing an existing system must not decrease its safety. The new European legislation also allows determining the adequate level of safety of a system by performing a similarity analysis with a reference system. Thus, the question about the adequate level of safety of new or changed systems is answered by a comparison. To be able to make this comparison with the codes of practice or another system the safety-related parts of the system have to be identified. However, many analysts have difficulties in distinguishing safety-related from non-safety-related system elements and rules. A reason for this is the presentation of system description and rules that is generally inappropriate for safety analysis. This presentation makes the analysis as well as the evaluation, assessment and approval of the system difficult.

The objective of this thesis is to provide the professionals involved in safety analysis and evaluation with a tool that facilitates this comparison.

For this purpose, the new term safety layer is introduced and clearly defined. The system's safety layers are the elements for a comparison of the safety of two systems. To facilitate a distinction between general safety measures and safety layers a catalogue of criteria is worked out. This catalogue is used to check whether a safety measure is a safety layer.

Within the scope of this thesis a new method is developed to facilitate a systematic identification of safety layers of a railway system: the ISES method. This new method is designed in such a way that it integrates into the process of analysing and demonstrating system safety.

The application of the ISES method and the advantage of identifying safety layers are demonstrated using a level crossing example. A validation is performed to examine whether the requirements for the intended use of the term safety layer and the ISES method are fulfilled. By looking at the interface between the results of the ISES method and accident analyses the circle of safety analysis is closed.

1 Einleitung

1.1 Motivation

Mobilität ist ein Grundbedürfnis unserer Gesellschaft. Der Schienenverkehr ist nach dem motorisierten Individualverkehr und dem öffentlichen Straßenpersonenverkehr die wichtigste Verkehrsart in Deutschland. Im Jahr 2009 fuhren in Deutschland rund 2,37 Milliarden Fahrgäste mit Eisenbahnen [Sta10]. Aufgrund der hohen Fahrgastzahlen werden an die Eisenbahn hohe Sicherheitsanforderungen gestellt. Durch das *Allgemeine Eisenbahngesetz (AEG)* sind die Eisenbahnen „verpflichtet, ihren Betrieb sicher zu führen und die Eisenbahninfrastruktur, Fahrzeuge und Zubehör sicher zu bauen und in betriebssicherem Zustand zu halten“ [Bun09, § 4 (1)].
Bevor Eisenbahnfahrzeuge und Eisenbahnanlagen in Betrieb genommen werden dürfen, benötigen sie eine Zulassung bzw. eine Inbetriebnahmegenehmigung oder Abnahme, z. B. durch das Eisenbahn-Bundesamt (EBA). Dadurch muss ein Eisenbahnunternehmen nicht nur seinen Betrieb sicher führen und seine Systeme sicher bauen, sondern es muss die Sicherheit seiner Systeme auch *nachweisen*. Dies gilt nicht nur für den Bau neuer Systeme, sondern auch für Änderungen an bestehenden Systemen.

1.1.1 Nachweis der Sicherheit mit Hilfe der anerkannten Regeln der Technik

Eine wichtige Rolle bei der Bewertung und dem Nachweis der Sicherheit eines Systems spielen die *anerkannten Regeln der Technik*. Die Eisenbahn-Bau- und Betriebsordnung (EBO) [Bun12] fordert in § 2 (1): „Bahnanlagen und Fahrzeuge müssen so beschaffen sein, dass sie den Anforderungen der Sicherheit und Ordnung genügen. Diese Anforderungen gelten als erfüllt, wenn die Bahnanlagen und Fahrzeuge den Vorschriften dieser Verordnung und, soweit diese keine ausdrücklichen Vorschriften enthält, *anerkannten Regeln der Technik* entsprechen.“ Auch im Rahmen der aktuellen europäischen Entwicklung einer *gemeinsamen Sicherheitsmethode (CSM)* für die Evaluierung und Bewertung von Risiken [Eur09] sind die anerkannten Regeln der Technik von Bedeutung (Abbildung 1.1). Sie sind ein Grundsatz zur Akzeptanz von Risiken. Gefährdungen gelten dann als ausreichend beherrscht und Risiken als ausreichend kontrolliert, wenn die anerkannten Regeln der Technik angewendet werden.
Die anerkannten Regeln der Technik liegen jedoch in der Regel in einer für die Sicherheitsnachweisführung ungünstigen Form vor. Es gibt eine Vielzahl von Regelwerken: Gesetze, Normen, Betreiber-Richtlinien, technische Spezifikationen, etc. Sie enthalten sowohl sicherheitsrelevante als auch nicht-sicherheitsrelevante Anforderungen, ohne jedoch zwischen diesen beiden Kategorien zu unterscheiden. Für den Nachweis der Sicherheit genügt es jedoch, die Einhaltung der sicherheitsrelevanten Anforderungen nachzuweisen. Werden sie nicht eingehalten, kann der Sicherheitsnachweis über das in Deutschland weit verbreitete und gesetzlich verankerte Risikoakzeptanzkriterium *Mindestens Gleiche Sicherheit (MGS)* geführt werden. Das Prinzip von MGS basiert auf der EBO: „Von den anerkannten Regeln der Technik darf abgewichen werden, wenn mindestens die gleiche Sicherheit wie bei Beachtung dieser Regeln nachgewiesen ist“ [Bun12, § 2 (2)].
Da in den Regelwerken jedoch nicht zwischen sicherheitsrelevanten und nicht-sicherheitsrelevanten Anforderungen unterschieden wird, muss die Frage, ob die Abweichung einen Einfluss auf die Sicherheit des Systems hat, stets aufs Neue beantwortet werden. Der Aufwand zur Beantwortung dieser Frage kann beträchtlich sein. Scheut der Hersteller diesen Aufwand, oder kann er die Frage nicht eindeutig beantworten, müssen die anerkannten Regeln der Technik eingehalten werden. Die

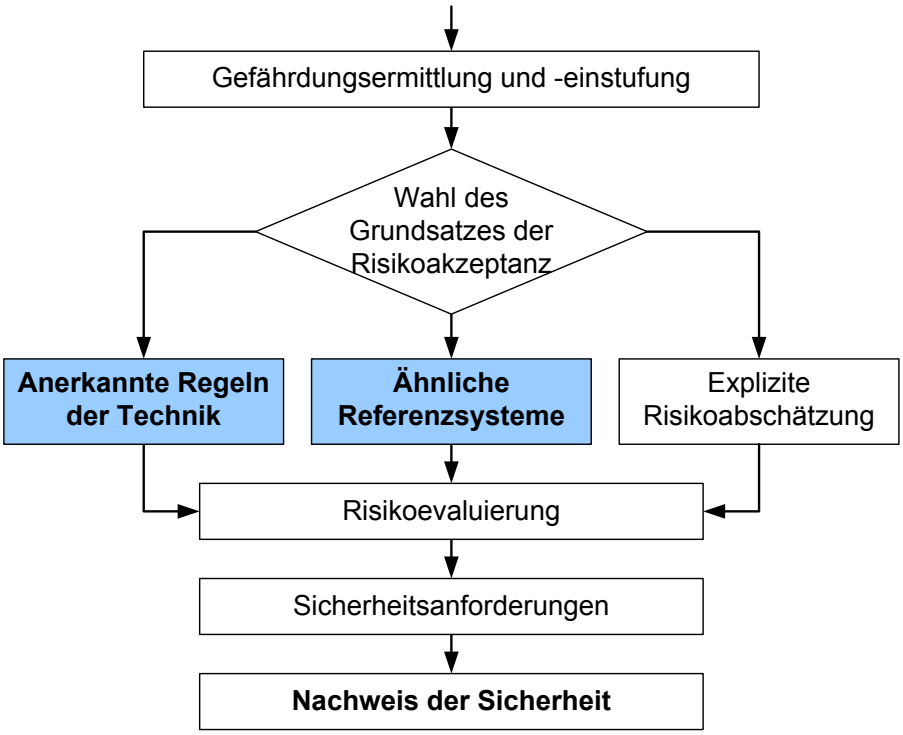

Abbildung 1.1: Auszug aus der gemeinsamen Sicherheitsmethode (CSM) für die Evaluierung und Bewertung von Risiken; blau: die im Rahmen der vorliegenden Arbeit näher betrachteten Zweige

Tatsache, dass der sicherheitsrelevante Teil der Anforderungen in den Regelwerken nicht explizit als solcher erkennbar ist, kann somit zu einem Innovationshemmnis werden.
Eine Identifikation und geeignete Darstellung des für die Sicherheit relevanten Teils der anerkannten Regeln der Technik könnte die Sicherheitsnachweisführung vereinfachen. Auswirkungen von Abweichungen von den anerkannten Regeln der Technik ließen sich einfacher und besser abschätzen, und die Nachweisführung würde transparenter und vergleichbarer. Dadurch könnten Innovationen gefördert und Kosten gespart werden.

1.1.2 Nachweis der Sicherheit durch einen Vergleich von Systemen

Ein weiterer Grundsatz der Risikoakzeptanz in der CSM[1] ist der *Vergleich mit ähnlichen Systemen* [Eur09]. Hierbei wird die Sicherheit eines neuen Systems mit der eines Referenzsystems verglichen (Abbildung 1.1). Das neue System gilt als ausreichend sicher, wenn es mindestens das gleiche Sicherheitsniveau erreicht wie das Referenzsystem.
Ein Sonderfall dieser Vorgehensweise ergibt sich, wenn das neue System durch eine *Änderung* des Referenzsystems entsteht. Dieser Aspekt gewinnt in Europa zunehmend an Bedeutung, denn Europa verfügt in weiten Teilen bereits über eine gut ausgebaute Eisenbahninfrastruktur und eine große Anzahl an bewährten Eisenbahnfahrzeugen. Erfahrene Hersteller entwickeln ihre Produkte – sowohl im Infrastruktur- als auch im Fahrzeugbereich – kontinuierlich weiter. Daher werden immer seltener Eisenbahnsysteme komplett neu entwickelt. Stattdessen werden an den bestehenden Systemen Änderungen vorgenommen, um sie z. B. an die geänderten Kundenwünsche oder den Stand der Technik

[1] Neben der gemeinsame Sicherheitsmethode für die Evaluierung und Bewertung von Risiken [Eur09] gibt es noch weitere gemeinsame Sicherheitsmethoden (CSM), z. B. für die Konformitätsbewertung in Bezug auf die Anforderungen an die Erteilung von Eisenbahnsicherheitsgenehmigungen und die Ausstellung von Eisenbahnsicherheitsbescheinigungen. Im Rahmen der vorliegenden Arbeit ist mit CSM jedoch stets die gemeinsame Sicherheitsmethode für die Evaluierung und Bewertung von Risiken [Eur09] gemeint.

anzupassen. Bei diesen Änderungen ist es wichtig, dass die Sicherheit des (Gesamt-)Systems erhalten bleibt oder ggf. noch erhöht wird. Gleichzeitig sollen durch die Änderungen möglichst geringe Kosten, insbesondere bei der Zulassung, entstehen. Zu diesem Zweck wird für das geänderte System eine sogenannte Delta-Betrachtung durchgeführt. Sie ist die Grundlage für den Vergleich mit dem alten System, das als Referenzsystem dient.
Für diesen Vergleich ist es notwendig, dass die sicherheitsrelevanten Teile beider Systeme identifiziert sind und in einer vergleichbaren Form vorliegen. Unterscheiden sich die beiden Systeme bzgl. ihrer Sicherheitsmaßnahmen oder anderer sicherheitsrelevanter Teile, dann muss nachgewiesen werden, dass das neue System mindestens das gleiche Sicherheitsniveau wie das Referenzsystem erreicht [Eur09]. Dabei muss dieser Vergleich nicht notwendigerweise quantitativ erfolgen.
Eine Identifikation und geeignete Darstellung des sicherheitsrelevanten Teils des Systems könnte auch diese Art der Nachweisführung erleichtern. Wie bei dem Vergleich mit den anerkannten Regeln der Technik ließen sich auch hier Aufwand und Kosten sparen und Innovationen fördern.

1.1.3 Nachweis der Sicherheit durch explizite Risikoabschätzung

Der dritte Grundsatz der Risikoakzeptanz in der CSM ist die *explizite Risikoabschätzung und -evaluierung* [Eur09] (Abbildung 1.1). Bei dieser Vorgehensweise werden Risiken „unter Berücksichtigung der vorhandenen Sicherheitsmaßnahmen quantitativ oder qualitativ beurteilt“ [Eur09]. Die Risiken gelten als tolerierbar, wenn sie kleiner oder gleich einem bestimmten Grenzrisiko sind. Dieses Grenzrisiko für ein Gesamtsystem (z. B. das System Eisenbahn) zu bestimmen, ist eine schwierige, gesellschaftspolitische Aufgabe. Für einzelne Bereiche wird das Grenzrisiko durch europäische oder nationale Vorschriften oder im einzelnen Anwendungsfall auch vom zuständigen Eisenbahnunternehmen festgelegt. Für eine quantitative Beurteilung der Risikoakzeptanz werden dabei z. B. die Prinzipien *As Low As Reasonably Practicable (ALARP)* oder *Minimum Endogenous Mortality (MEM)* [DIN00] verwendet. Neben der Bestimmung des Grenzrisikos müssen auch die Risiken des betrachteten Systems unter Berücksichtigung der Umgebungsbedingungen und des geplanten Betriebs explizit bestimmt werden (siehe z. B. PROFUND-Methode [Slo06]).
Bei sehr schwerwiegenden Folgen von Systemausfällen wird zur Risikoakzeptanz statt einer expliziten Angabe des Risikos häufig eine Ausfall- bzw. Gefährdungsrate verwendet und mit einer tolerierbaren Ausfall- bzw. Gefährdungsrate verglichen (siehe z. B. [Eur09] und [DIN03]).

1.2 Ziel

Das Ziel der vorliegenden Arbeit ist es, begriffliche und methodische Mittel zur Verfügung zu stellen, um zwei der drei in der CSM aufgeführten Möglichkeiten zur Risikoakzeptanz und Sicherheitsnachweisführung – mit Hilfe der anerkannten Regeln der Technik und mit Hilfe von Referenzsystemen (Abbildung 1.1) – zu unterstützen. In beiden Fällen liegt die Schwierigkeit jeweils im sicherheitsbezogenen Vergleich – zwischen dem neuen System und den anerkannten Regeln der Technik oder einem Referenzsystem. Aber auch verschiedene Möglichkeiten der Veränderung eines Systems sollen bzgl. ihrer Sicherheit möglichst einfach und pragmatisch miteinander verglichen werden können. Wichtig hierbei ist, dass ein solcher Vergleich nicht nur den Sicherheits- und Systemexperten vorbehalten bleibt. Vielmehr ist es in der (Weiter-)Entwicklung eines Systems von großer Bedeutung, dass eine verständliche Vergleichsmöglichkeit zwischen verschiedenen Systemvarianten von Entwicklern, Betreibern, Managern, Finanzfachkräften und Behörden als Entscheidungsgrundlage genutzt werden kann.
Um diesen Vergleich zu ermöglichen, wird der Begriff *Sicherheitsschicht* neu eingeführt. Obwohl das Wort Sicherheitsschicht im Eisenbahnbereich bereits vorgestellt wurde [SP07], existiert bislang noch keine klare Definition dieses Begriffs. Daher besteht das erste Teilziel der vorliegenden Arbeit darin, eine geeignete *Definition* seines Begriffsinhalts zu erarbeiten. Sicherheitsschichten sind eine

Kombination von technischen, funktionalen und organisatorischen Sicherheitsmaßnahmen, die als zusammenhängende Einheit betrachtet werden. Sie bilden eine Möglichkeit der durchgängigen Darstellung von Sicherheitsmaßnahmen, durch die der sicherheitsbezogene Vergleich von Systemen und Regeln vereinfacht werden kann.
Das zweite Teilziel der vorliegenden Arbeit besteht in der Entwicklung einer *neuen Methode*, um die Sicherheitsschichten eines Systems zu identifizieren, sodass ein *Modell der Sicherheitsschichten* für dieses System erstellt werden kann. Durch ein Modell der Sicherheitsschichten lassen sich die Sicherheitsmaßnahmen eines Systems explizit und in einer für die Sicherheitsnachweisführung geeigneten Weise darstellen. Die Unterschiede zu den anerkannten Regeln der Technik oder einem Referenzsystem werden sichtbar, die einzelnen Sicherheitsschichten können mit konkreten Anforderungen verglichen werden und die Nachweisführung wird dadurch erleichtert. Das Konzept der Sicherheitsschichten lässt sich sowohl auf geplante und existierende Systeme als auch auf Regelwerke und anerkannte Regeln der Technik anwenden. Sowohl bei der Definition des Begriffs Sicherheitsschicht als auch bei der Entwicklung der neuen Methode werden die besonderen Rahmenbedingungen des Eisenbahnbereichs, die dort üblichen Vorgehensweisen und insbesondere die Anforderungen der CENELEC-Normen berücksichtigt.
Die neue Methode soll nicht nur die Sicherheitsschichten des untersuchten Systems identifizieren, sondern auch einen Beitrag zur Identifikation der Sicherheitsschichten des gesamten Eisenbahnsystems leisten. Auf diese Weise kann auf lange Sicht ein Modell der Sicherheitsschichten des Eisenbahnsystems erstellt werden. Es handelt sich hierbei um Grundlagenarbeit, die viele nachfolgende Analysen – insbesondere aus dem Bereich der Sicherheitsnachweisführung – vereinfachen kann. Derartige Grundlagenarbeit gab es bereits in verschiedenen Domänen. Im Bereich der Eisenbahn z. B. bzgl. der Gefährdungsidentifikation: Im Projekt Eurointerlocking [DM07] wurde eine generische Gefährdungsliste[2] für Stellwerkssysteme erstellt. Der Aufwand für eine solche Grundlagenarbeit ist hoch. Zum einen muss eine konsistente methodische Basis geschaffen werden, zum anderen ist das Eisenbahnsystem ein sehr großes und komplexes System, sodass für die Analyse ein hoher Arbeitsaufwand besteht. Der hohe Aufwand ist ein wesentlicher Grund dafür, warum die bisher durchgeführten Grundlagenarbeiten oft nur für kleine Bereiche des Eisenbahnsystems durchgeführt wurden und teilweise auch nicht bis zu Ende geführt wurden.
Mit der neuen Methode soll die methodische Basis für diese Grundlagenarbeit geschaffen werden. Durch die Anwendung der Methode können nach und nach immer mehr Sicherheitsschichten des Eisenbahnsystems identifiziert werden, wodurch der Aufwand zur Erstellung eines Modells der Sicherheitsschichten des Eisenbahnsystems gering gehalten werden kann.

1.3 Struktur der vorliegenden Arbeit

Die vorliegende Arbeit gliedert sich wie folgt (siehe auch Abbildung 1.2):
In Kapitel 2 werden zunächst *verbreitete Begriffe und Konzepte* zum Thema Sicherheit aus verschiedenen Domänen erläutert. Diese Begriffe und Konzepte bilden die Basis für die nachfolgenden Kapitel. Das Kapitel erläutert die Zusammenhänge zwischen den Begriffen und die Unterschiede zwischen den Domänen. Auf diese Weise wird ein Überblick über den Stand der Wissenschaft und Technik in Bezug auf Sicherheitsschichten und verwandte Bereiche gegeben.
In Kapitel 3 wird der zentrale Begriff dieser Arbeit definiert und erläutert: der Begriff der *Sicherheitsschicht*.
Kapitel 4 gibt einen Überblick über gängige *Modelle und Darstellungsweisen* für Begriffe aus dem Umfeld der Sicherheitsschichten. Die vorgestellten Darstellungsweisen aus den verschiedenen Domänen werden bzgl. ihrer Eignung zur Darstellung von Sicherheitsschichten bewertet und verglichen.

[2] Die Gefährdungsliste wird in [DM07] als Gefahrenliste oder Hazard-List bezeichnet. In der vorliegenden Arbeit werden die Begriffe Gefahr und Gefährdung als synonym betrachtet. Es wird die Benennung Gefährdung bevorzugt.

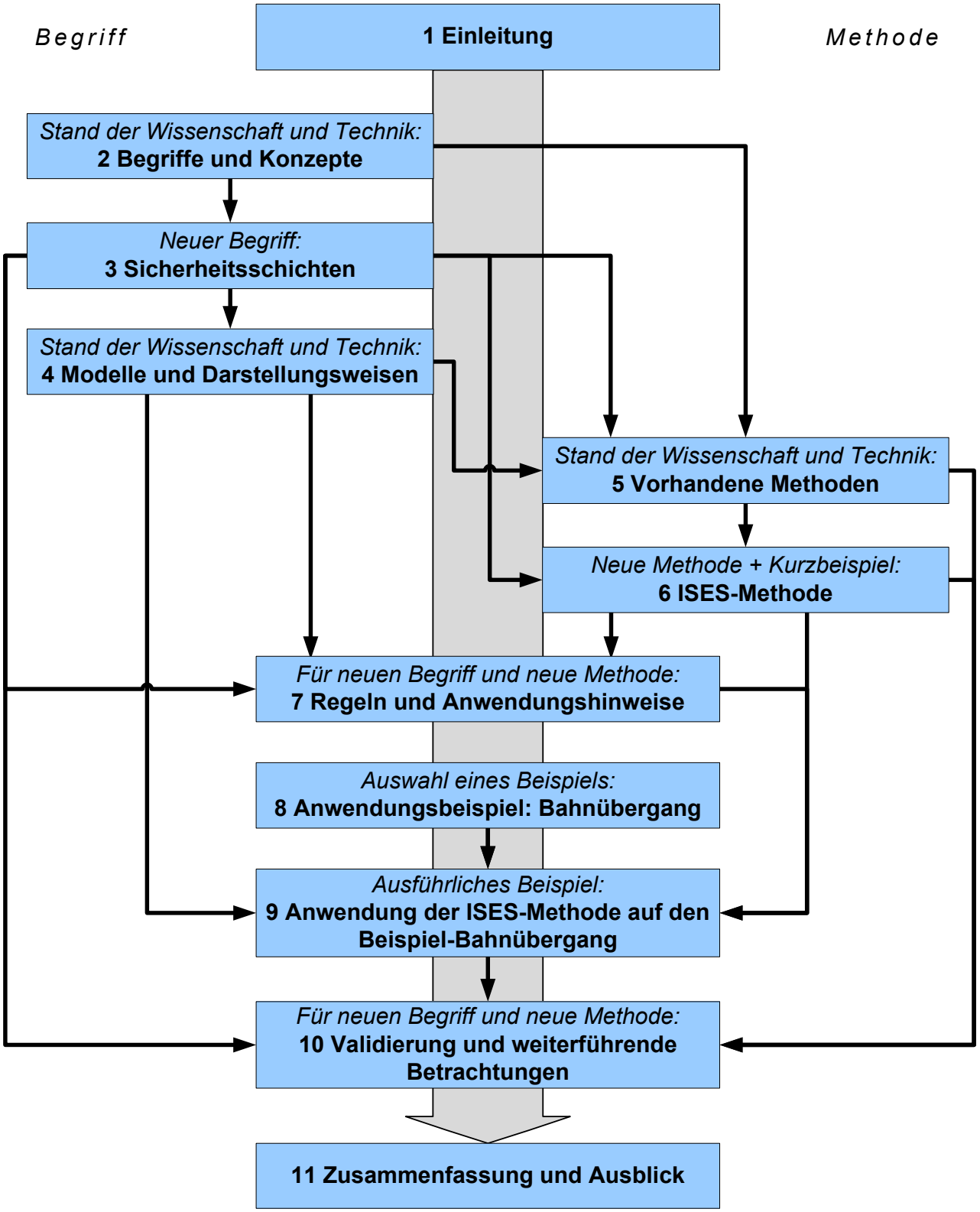

Abbildung 1.2: Struktur der vorliegenden Arbeit

Als Ergebnis wird ein geeignetes Modell zur Darstellung von Sicherheitsschichten ausgewählt.
Kapitel 5 beginnt mit einer Definition von Anforderungen an eine *Methode zur Identifikation von Sicherheitsschichten*. Anschließend wird eine Auswahl von potenziell geeigneten, vorhandenen Methoden aus verschiedenen Domänen vorgestellt, die für die Identifikation von Sicherheitsschichten anwendbar sein könnten. Diese Methoden werden verglichen sowie ihre Stärken und Schwächen beleuchtet.
In Kapitel 6 wird eine *neue Methode* zur Identifikation von Sicherheitsschichten vorgestellt: die *Methode zur Identifikation von Sicherheitsschichten in Eisenbahnsystemen (ISES-Methode)*. Die ISES-Methode kombiniert mehrere der vorhandenen Methoden aus Kapitel 5, ergänzt sie, spezialisiert sie für die Domäne Eisenbahn und für den Zweck der Identifikation von Sicherheitsschichten und füllt die Lücken zwischen ihnen.
Kapitel 7 gibt dem Anwender *Regeln* für den korrekten Umgang mit Sicherheitsschichten an die Hand. Diese Regeln betreffen unter anderem die korrekte Darstellung von Sicherheitsschichten und die Anwendung der ISES-Methode.
In Kapitel 8 wird ein *Bahnübergang* als *Beispiel* für eine ausführliche Anwendung der ISES-Methode vorgestellt. Zunächst wird ein Überblick über verschiedene gängige Bahnübergangstypen gegeben, von denen ein Typ als Beispiel ausgewählt und beschrieben wird. Anschließend wird eine relevante Gefährdung ausgewählt, anhand derer ein Modell der Sicherheitsschichten für den Beispiel-Bahnübergang aufgestellt werden soll.
In Kapitel 9 wird die ISES-Methode aus Kapitel 6 auf das in Kapitel 8 beschriebene Beispiel, den Bahnübergang, *angewendet*. Die einzelnen Schritte der ISES-Methode werden durchgeführt und ausführlich erläutert. Als Ergebnis liefert die ISES-Methode sowohl ein Modell der Sicherheitsschichten für das Beispiel und die ausgewählte Gefährdung als auch eine Grundlage für die Durchführung weiterer Analysen mit der ISES-Methode in Form einer Checkliste. Anschließend wird Nutzen der ISES-Methode und des Modells der Sicherheitsschichten anhand einer Veränderung des Beispiel-Bahnübergangs durch die Einführung des *European Train Control System (ETCS)* dargestellt.
Kapitel 10 widmet sich der *Validierung* des Begriffs Sicherheitsschicht und der ISES-Methode. Es wird analysiert, ob der neue Begriff Sicherheitsschicht und die neue ISES-Methode alle an sie gestellten Anforderungen erfüllen. Anschließend wird anhand einer Why-Because-Analyse eines Beinahe-Unfalls gezeigt, wie sich das Modell der Sicherheitsschichten in bestehende Konzepte aus dem Bereich der Unfallanalyse einfügt.
Kapitel 11 fasst die Ergebnisse dieser Arbeit zusammen und gibt einen Ausblick auf weitere Aufgaben, die in der vorliegenden Arbeit nicht behandelt werden konnten.

2 Verbreitete Begriffe und Konzepte

Dieses Kapitel erläutert Begriffe und Konzepte aus verschiedenen Domänen rund um das Thema Sicherheitsschichten. Zunächst werden die grundlegenden Begriffe aus dem Bereich der Sicherheit erläutert. Diese Begriffe bilden die Basis für die folgenden Kapitel. Für die grundlegenden Begriffe aus dem Bereich der Sicherheit gibt es in den verschiedenen Domänen und verschiedenen Fachbereichen zahlreiche eigene, voneinander abweichende Definitionen. Daher ist es vor Beginn jeder Arbeit, jeder Analyse und jeder Diskussion wichtig, die verwendeten Fachbegriffe klar zu definieren. Dazu werden im Rahmen dieser Arbeit – soweit möglich und sinnvoll – Begriffe aus Normen verwendet. Ihre Begriffsdefinitionen sind allgemein zugänglich und weit verbreitet und entsprechen somit in der Regel[1] als anerkannte Regeln der Technik dem in der Domäne üblichen Verständnis.
Die vorliegende Arbeit ist aus dem Blickwinkel der Eisenbahn entstanden. Die ausgewählten Begriffe und ihre Definitionen sind in diesem Kontext zu betrachten. Neben den Begriffen aus dem Umfeld der Eisenbahn werden im Folgenden noch weitere Begriffe aus anderen Domänen angegeben. Dadurch wird deutlich, dass das Thema Sicherheit in vielen Domänen behandelt wird und dass dabei durchaus ähnliche Konzepte genutzt werden. Der Sprachgebrauch ist in den unterschiedlichen Domänen jedoch nicht einheitlich, wodurch es zu Schwierigkeiten beim Übertragen von Konzepten von einer Domäne auf die andere kommen kann. Insbesondere soll durch die im Folgenden vorgestellten Begriffe verdeutlicht werden, wie wichtig eine klare Begriffsdefinition ist. Zunächst werden jedoch die für die vorliegende Arbeit wichtigsten Normen vorgestellt.

2.1 Normen

Die wichtigsten Normen bzgl. Eisenbahnsicherheit, insbesondere im Bereich der Signaltechnik, sind:

- DIN EN 50126-1[2]: Spezifikation und Nachweis der Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit und Sicherheit (RAMS) Teil 1: Grundlegende Anforderungen und genereller Prozess [DIN00]
- DIN EN 50128: Software für Eisenbahnsteuerungs- und Überwachungssysteme [DIN12]
- DIN EN 50129: Sicherheitsrelevante elektronische Systeme für Signaltechnik [DIN03]

Die DIN EN 50126-1 [DIN00] beschreibt einen generellen Lebenszyklus für alle Arten von Bahnsystemen: vom Konzept bis zur Stilllegung des Systems. Die DIN EN 50128 [DIN12] definiert Anforderungen an die Entwicklung und Wartung von Software in Eisenbahnsystemen. Die DIN EN 50129 [DIN03] legt die Struktur des Sicherheitsnachweises fest, der für sicherheitsrelevante Signaltechnik erstellt werden muss.
Ohne die Normen EN[3] 50126-1 und EN 50129 wird heute in Europa kaum noch ein sicherheitsbezogenes System entwickelt und zugelassen, das in der Eisenbahn-Signaltechnik Verwendung finden

[1] Normen können veralten und gehören dann nicht mehr zu den anerkannten Regeln der Technik.

[2] Die DIN EN 50126-1 [DIN00] ist die deutsche Fassung der EN 50126 [CEN99], die 2006 durch die Berichtigung [DIN06] in DIN EN 50126-1 umbenannt wurde. Die Umbenennung erfolgte, um Platz für die Teile 2 (Leitfaden zur Anwendung der EN 50126-1 für Sicherheit, [CEN07]) und 3 (Leitfaden zur Anwendung der EN 50126-1 für Bahnfahrzeuge RAM, [CEN08]) zu schaffen. Da die Teile 2 und 3 bisher nicht als Norm veröffentlicht wurden, wird im Sprachgebrauch oft noch die alte Bezeichnung DIN EN 50126 verwendet.

[3] Mit EN statt mit DIN EN wird eine europäische Norm dann bezeichnet, wenn man sie im (europäischen) internationalen Kontext referenziert. Dabei wird davon ausgegangen, dass sich die verschiedenen länderspezifischen Versionen der Norm, also DIN EN, BS EN, NF EN etc. nur durch ihre Sprache, nicht aber in ihrem Inhalt unterscheiden. Diese Annahme ist leider nicht immer ganz richtig.

soll. Und auch außerhalb Europas werden diese Normen immer häufiger eingesetzt.
Die drei Normen EN 50126-1, EN 50128 und EN 50129 zusammen werden üblicherweise auch als „die CENELEC-Normen“ bezeichnet, da sie alle vom europäischen Komitee für elektrotechnische Normung (CENELEC) herausgegeben wurden. Die CENELEC-Normen stammen aus den Jahren 1999 – 2012und befinden sich derzeit in Überarbeitung.
Eine weitere Norm, die gelegentlich im Bahnbereich Anwendung findet, ist die DIN EN 61508. Sie ist eine domänenübergreifende Norm, die auch als „Mutter der Sicherheitsnormen“ bezeichnet wird. Sie besteht aus sieben Teilen: DIN EN 61508-1 [DIN11a] bis DIN EN 61508-7 [DIN11c]. Die DIN EN 61508 ist eine Norm, die auf elektrische / elektronische / programmierbar elektronische Systeme (E/E/PE Systeme) immer dann anzuwenden ist, wenn diese Systeme zur Ausführung von Sicherheitsfunktionen eingesetzt werden und für den Anwendungsbereich keine sektorspezifische Norm vorliegt. Sie versteht sich als Basisnorm, die für die verschiedenen Anwendungsgebiete die Entwicklung einer entsprechenden internationalen Norm erleichtern soll. Für Telekommunikations-, Signal- und Datenverarbeitungssysteme der Eisenbahnen gibt es eine sektorspezifische Normenfamilie: die CENELEC-Normen. Es kommt jedoch vor, dass generische E/E/PE Komponenten, wie z. B. speicherprogrammierbare Steuerungen (SPS), die nach der DIN EN 61508 entwickelt wurden, im Bahnbereich verwendet werden sollen. Dann muss der Lebenszyklus nach DIN EN 61508 in den Lebenszyklus gemäß den CENELEC-Normen integriert werden. Dadurch wird die DIN EN 61508 auch für den Bahnbereich relevant.
Die DIN EN 61511 ist der sektorspezifische Zuschnitt der DIN EN 61508 auf die Prozessindustrie. Sie behandelt die funktionale Sicherheit sicherheitstechnischer Systeme für die Prozessindustrie und besteht aus drei Teilen: DIN EN 61511-1 [DIN05a] bis DIN EN 61511-3 [DIN05b]. Da der Gedanke an Sicherheitsmaßnahmen zur Vermeidung von Unfällen auch im Bereich der Prozessindustrie weit verbreitet ist, sollen an einigen Stellen auch Begriffe aus dieser Norm aufgeführt werden.

2.2 Basisbegriffe

Die im Folgenden aufgeführten Basisbegriffe entstammen zum größten Teil den oben genannten Normen. Schnieder weist in [Sch09] darauf hin, dass terminologische Festlegungen in Normen teilweise Fehler enthalten und bisweilen synonyme oder gar widersprüchliche Definitionen verwendet werden. Trotz dieser Mängel, werden für die vorliegende Arbeit – soweit möglich – Definitionen aus Normen verwendet. Sie stellen den allgemeinen Sprachgebrauch unter den Ingenieuren aus dem Bereich der (Eisenbahn-)Sicherheit dar. Dadurch wird die Verständlichkeit der vorliegenden Arbeit verbessert und die Übertragung in die Praxis vereinfacht.

System „Menge von Teilsystemen, die entsprechend einem Entwurf zusammenwirken“ [DIN03, 3.1.62]

Funktion „Art von Aktion oder Tätigkeit, durch die ein Produkt seinen beabsichtigten Zweck erfüllt“ [DIN03, 3.1.20]

Schaden „physische Verletzung oder Schädigung der Gesundheit von Menschen oder Schädigung von Gütern oder der Umwelt“ [DIN11b, 3.1.1]

Unfall „Ein nicht beabsichtigtes Ereignis oder eine Reihe von Ereignissen mit der Folge von Toten, von Verletzten, des Verlustes eines Systems oder von Umweltschäden“ [DIN03, 3.1.1][4]

Gefahr „Eine physikalische Situation, die potentiell einen Schaden für den Menschen beinhaltet“ [DIN00, 3.17]. Wird oft als Synonym für Gefährdung verwendet[5].

Gefährdung „Bedingung, die zu einem Unfall führen kann“ [DIN03, 3.1.21]. Wird oft (wie auch in der vorliegenden Arbeit) als Synonym für Gefahr verwendet[5].

[4] Zu den Folgen eines Unfalls gehören auch Sachschäden, auch wenn dies in [DIN03] nicht explizit erwähnt wird.

[5] Ein Grund für die synonyme Verwendung der Begriffe Gefahr und Gefährdung liegt darin, dass beide in der englischen Fassung der jeweiligen Normen als „hazard“ bezeichnet werden.

Risiko „Kombination aus Häufigkeit oder Wahrscheinlichkeit und den Folgen eines spezifizierten gefährlichen Ereignisses“ [DIN03, 3.1.43]

Risikominderung Minderung der Häufigkeit / Wahrscheinlichkeit oder Minderung der Folgen eines spezifizierten gefährlichen Ereignisses

Sicherheit (safety) „Das Nichtvorhandensein eines unzulässigen Schadensrisikos“ [DIN00, 3.35]. Spricht man von Sicherheit im Sinne von *safety*, so ist stets der Schutz vor *unabsichtlichen*, *ungeplanten* gefährlichen Ereignissen, wie z. B. Unfällen, gemeint. Sicherheit bzgl. *absichtlich* herbeigeführter schädlicher Ereignisse wird im Englischen hingegen als *security* bezeichnet (siehe Sicherheit (security)).

Sicherheit (security) Sicherheit im Sinne des Wachschutzes, d. h. Schutz vor Sachbeschädigung (Vandalismus), terroristischen Anschlägen, unerlaubtem Betreten, Spionage, kurz: Schutz gegen Schaden, der durch absichtliches menschliches Handeln entsteht. Der Begriff *security* beschreibt auch die Sicherheit im militärischen Sinne.

sicherheitsrelevant „trägt Sicherheitsverantwortung“ [DIN03, 3.1.56]

Sicherheitsintegritätslevel (SIL) „Eine von einer festgelegten Anzahl diskreter Stufen für die Spezifizierung der ausreichenden Sicherheit von Sicherheitsfunktionen, die sicherheitsrelevanten Systemen zugeordnet sind“ [DIN00, 3.38]. Die DIN EN 50129 [DIN03] definiert die SIL 0, 1, 2, 3 und 4.

unerwünschtes Ereignis Ein Ereignis, dessen Eintreten unerwünscht ist und daher vermieden werden soll. Zu den unerwünschten Ereignissen zählen in der Regel Unfälle, gefährliche Vorfälle sowie Ereignisse, die das Risiko für das Auftreten der beiden genannten erhöhen.

Fehlzustand (engl. error) „Abweichung vom beabsichtigten Entwurf, die zu unerwünschtem Systemverhalten oder Ausfall führen kann“ [DIN03, 3.1.15]. Fehlzustände können zulässig (tolerierbar) oder unzulässig sein. Unzulässige Fehlzustände können zu Gefährdungen führen.

Fehlfunktion / Fehler (engl. failure[6]) „Abweichung vom spezifizierten Verhalten des Systems. Eine / ein Fehlfunktion / Ausfall ist die Folge einer Fehlerursache (fault) oder eines Fehlzustandes (error) im System“ [DIN03, 3.1.17]

Ausfall (engl. fault[6]) 1. Ereignis: „Beendigung der Funktionsfähigkeit einer materiellen Einheit im Rahmen der zugelassenen Beanspruchung“ [DIN90b, 2.2.4]. 2. Zustand: „Abnormaler Zustand, der zu einem Fehler oder einer Fehlfunktion / Ausfall in einem System führen kann“ [DIN03, 3.1.18]

menschliches Versagen „Menschliche Handlung, die zu einem ungewollten Verhalten des Systems oder zu einer Fehlfunktion führen kann“ [DIN03, 3.1.24]

sicherer Zustand „Zustand, der die Sicherheit weiterhin bewahrt“ [DIN03, 3.1.44]

Eine Möglichkeit der Darstellung der Zusammenhänge zwischen den Begriffen aus dem Bereich der Sicherheit ist das Verfügbarkeits-Sicherheitsdiagramm (Abbildung 2.1). Die durchgezogenen Pfeile geben dabei mögliche Zustandsübergänge an. Da sich nicht alle der oben aufgeführten Begriffe in einer Grafik veranschaulichen lassen, muss das Diagramm auf einige ausgewählte Begriffe beschränkt werden. Weitere Informationen über die Zusammenhänge dieser und anderer Begriffe aus dem Gebiet der Verlässlichkeit (Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit, Sicherheit (RAMS)) finden sich bei Laprie [Lap92] und Drewes [Dre09].

Sicherheit als akzeptables Risiko

Sicherheit als Nichtvorhandensein eines unzulässigen Risikos zu definieren ist ein relativ neuer Ansatz. Sicher bedeutet hier stets „sicher genug“. Die erforderliche Sicherheit leitet sich aus dem tatsächlich bestehenden und dem akzeptablen Risiko ab. Zugleich wird anerkannt, dass immer ein Restrisiko

[6] Die englische Übersetzung ist hier angegeben zur Unterscheidung der beiden Bedeutungen des deutschen Wortes „Ausfall“

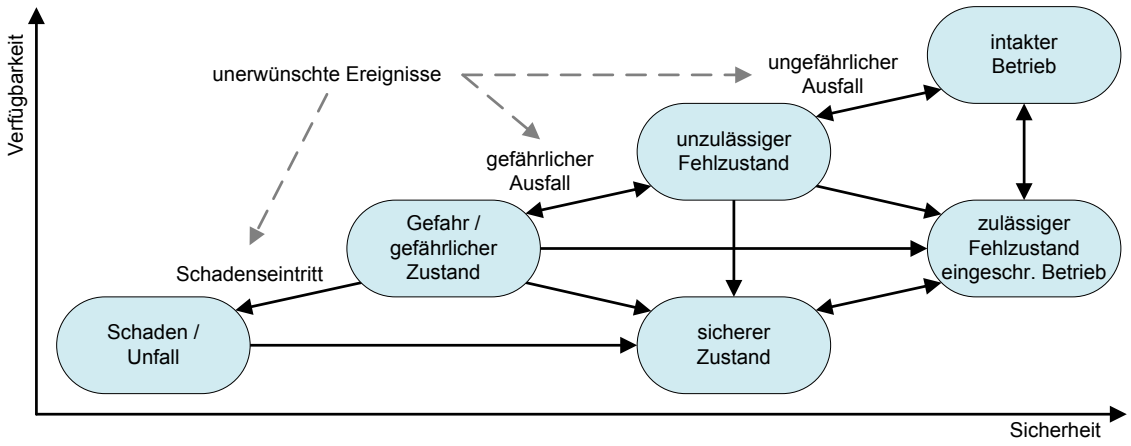

Abbildung 2.1: Zustände eines technischen Systems im Verfügbarkeits-Sicherheitsdiagramm in Anlehnung an Schnieder [Sch03]

besteht, und dass dieses Restrisiko nicht vollständig eliminiert werden kann und somit akzeptiert werden muss und kann. Die CENELEC-Normen lösen damit die Denkweise älterer Regelwerke ab, in denen Sicherheit als absoluter Zustand angesehen wurde. Nach der damaligen Philosophie war ein System entweder sicher oder nicht sicher. Sicher bedeutete soviel wie „Es kann nichts passieren“ und „Es ist nicht nötig, mehr für die Sicherheit zu tun“. Diese Sicherheit wurde durch das Einhalten bestimmter Regeln erreicht. Es wurde nicht zwischen mehr oder weniger sicher unterschieden. Über das stets bestehende Restrisiko wurde nicht gesprochen. Ein Restrisiko bedeutet, dass Menschen verletzt oder getötet werden könnten, und dass man bereit ist, eine gewisse Anzahl von Toten zu akzeptieren. Dieser Gedanke war vielen Menschen so fremd, dass es rechtliche Probleme mit dieser Tatsache gab und auch heute noch gibt.
Ein Hersteller / Betreiber müsste nach der vormaligen Philosophie eigentlich jedwedes Risiko, das ihm bekannt ist, beseitigen. Dass Betreiber (und mit ihnen die Gesellschaft) bereit sind, eine gewisse Anzahl von Toten zu akzeptieren, ist einen Tatsache, denn jedes Jahr sterben Menschen im Eisenbahnverkehr (z. B. 167 im Jahr 2004 in Deutschland) und der Eisenbahnbetrieb läuft trotzdem weiter. Diese Tatsache auszusprechen, ruft vielerorts Empörung hervor. Doch genau dieses verbleibende, akzeptable Restrisiko zu bestimmen und zu benennen – sei es qualitativ oder quantitativ – fordert der risikoorientierte Sicherheitsansatz der CENELEC-Normen.

2.3 Begriffe aus dem Umfeld der Sicherheitsschichten

Der Begriff *Sicherheitsschicht* (safety layer) wurde im Rahmen eines Forschungsprojekts zur Entwicklung des „Modells der Sicherheitsschichten“ (MoSiS) im Eisenbahnsystem eingeführt [PSM07]. Die Bedeutung des Begriffs wird in [PSM07] grob umrissen als eine Kombination aus Technik und Prozeduren, Komponenten, Regeln und Personen, die als zusammenhängende Einheit interpretiert werden. Der Zweck von Sicherheitsschichten wird allgemein beschrieben als „Schutz des Systems und der ihm ausgesetzten Menschen, Mindern der Risiken, Abwenden von Gefahren, Abfangen von Fehlern [und] Verhindern von Unfällen"[SP07]. Sicherheitsschichten sollen kombinierbar und austauschbar sein [PSM07]. Eine eindeutige und klare Definition des Inhalts des Begriffs Sicherheitsschicht wurde bisher jedoch nicht erarbeitet. Die vorliegende Arbeit schließt diese Lücke.
Auch außerhalb des Eisenbahnbereichs findet sich die prinzipielle Idee von Sicherheitsschichten in der Literatur wieder. Je nach Anwendungsgebiet sind die Konzepte leicht unterschiedlich und unterscheiden sich auch in der Bezeichnung. Auf der Suche nach einer geeigneten Beschreibung des Konzepts der Sicherheitsschichten wurde in der Literatur nach geeigneten oder zumindest ähnlichen Begriffen

und Konzepten gesucht, mit dem Ziel, vorhandene Konzepte auf den konkreten Anwendungsfall für die Eisenbahn zu übertragen. Aus der Literaturrecherche ergibt sich, dass ähnliche Konzepte weit verbreitet, aber nicht vereinheitlicht sind. In diesem Abschnitt werden die geeignetsten Begriffe vorgestellt, um sie als Basis für die Definition des Begriffs Sicherheitsschicht verwenden zu können. Als Kriterium für die Auswahl der Begriffe wurde dabei ihre Eignung zur Umsetzung der Beschreibungen des Begriffs Sicherheitsschicht aus [PSM07] und [SP07] verwendet (siehe oben). Des Weiteren bilden die im Folgenden vorgestellten Begriffe die Basis für das Verständnis der Methoden aus Abschnitt 5.2.

2.3.1 (Sicherheits-)Barriere

Unter einer Barriere versteht man im allgemeinen Sprachgebrauch eine Sperre oder eine Schranke – also etwas, das den Durchgang verwehrt (Abbildung 2.2) oder etwas aufhält, z. B. ein austretendes Gas. Ausgehend von dieser Bedeutung haben sich in verschiedenen Domänen zahlreiche unterschiedliche Definitionen des Begriffs Barriere entwickelt. Oft, so wie auch in dieser Arbeit, wird das Wort *Barriere* als Kurzform für Sicherheitsbarriere verwendet. Ein guter Überblick über die verschiedenen Begriffe und ihre Definitionen wurde von Sklet in [Skl06] zusammengestellt.

Abbildung 2.2: Barriere

Das Konzept der Barrieren wird in vielen Industriezweigen genutzt, um Risikoreduktionsmaßnahmen zu beschreiben. Insbesondere in der chemischen Industrie, in der Prozessindustrie und im Bereich der Kraftwerkstechnik wird dieses Konzept verwendet. Auch im Eisenbahnbereich wird mittlerweile immer häufiger von Barrieren gesprochen: Das Projekt Rail Optimisation Safety Analysis (ROSA) z. B. verwendet Barrieren, um das Sicherheitsverhalten eines gesamten nationalen Bahnsystems zu erfassen und zu analysieren [SGPS10]. Wenn der Begriff Barriere im Bahnbereich verwendet wird, dann geschieht das meist ohne eine genaue Definition. Barriere wird stattdessen schlicht als Synonym für Sicherheitsmaßnahme verwendet [GHS$^+$09]. Dabei gibt es im Bahnbereich, im technischen Bericht CLC/TR 50126-2 [CEN07], durchaus eine Definition des Begriffs Sicherheitsbarriere (safety barrier): „a system or action, intended to reduce the rate of a hazard or a likely accident arising from the hazard and / or mitigate the severity of the likely accident“ [CEN07, 3.2.18].
Sklet hat die verschiedenen Definitionen für den Begriff Sicherheitsbarriere aus den verschiedenen Domänen und Anwendungsbereichen verglichen und daraus eine einheitliche Definition entwickelt: „Safety barriers are physical and / or non-physical means planned to prevent, control, or mitigate undesired events or accidents“ [Skl06]. Die Definition aus dem Bahnbereich (aus CLC/TR 50126-2 [CEN07]) passt zu Sklets Definition einer Sicherheitsbarriere. Da Sklets Definition jedoch präziser ist, soll in der vorliegenden Arbeit die Definition von Sklet, übersetzt ins Deutsche, verwendet werden:

Sicherheitsbarrieren sind physische und / oder nicht-physische Mittel, die geplant wurden, um unerwünschte Ereignisse oder Unfälle zu vermeiden, zu beherrschen oder abzumildern [Skl06]. Erläuterungen zu dieser Definition:

- *unerwünschtes Ereignis* (undesired event), auch gefährliches Ereignis genannt, kann z. B. ein Ausfall einer technischen Komponente, ein menschlicher Fehler, ein externes Ereignis oder eine Kombination davon sein
- *Unfall* (accident) ist ein unerwünschtes und ungeplantes Ereignis, das zu Toten, Verletzten, Umweltschäden und / oder materiellen Schäden führt
- *Mittel* (means) können sein: einzelne technische Komponenten oder menschliche Handlungen bis hin zu komplexen Systemen, die aus mehreren Menschen und Technologien bestehen
- *geplant* (planned) meint, dass mindestens ein Zweck des eingesetzten Mittels darin besteht, das Risiko zu reduzieren (es kann noch weitere Zwecke haben)
- *vermeiden* (prevent) bedeutet, die Wahrscheinlichkeit, mit der das unerwünschte / gefährliche Ereignis eintritt, zu verringern
- *beherrschen* (control) bedeutet, die (räumliche) Ausdehnung oder die Dauer des gefährlichen Ereignisses zu begrenzen, um eine Eskalation zu verhindern
- *abmildern* (mitigate) bezieht sich auf die Folgen des gefährlichen Ereignisses und bedeutet, das Ausmaß dieser Folgen zu reduzieren

2.3.2 Verteidigung / Abwehr / Schutz (Defence)

Verteidigung / Abwehr / Schutz (*defence*) ist ein Begriff, der seinen Ursprung im militärischen Bereich hat. Er ist in zahlreiche andere Domänen übertragen worden, z. B. in die Bereiche der Kernenergie und Datensicherheit. *Defence* (die deutsche Übersetzung ist eher unüblich) bezeichnet nach Reason [Rea04] die verschiedenen Mittel zur Erlangung von Sicherheit oder Schutz (protection) für Personen und Anlagen. Der Begriff wird vor allem im Zusammenhang mit dem Konzept der *Defence-in-Depth* (siehe unten) benutzt. Im Folgenden wird *Defence* ausschließlich im nicht-militärischen Sinn verwendet.

In die Tiefe gestaffelte Abwehr / Schutz (Defence-in-Depth)

Defence-in-Depth [Int96], zu Deutsch etwa „in die Tiefe gestaffelte Abwehr“ [Int94], ist ein Konzept, das u. a. im Bereich der Kernenergie verwendet wird. Es verfolgt die Strategie, Unfälle nach Möglichkeit zu verhindern, oder zumindest die möglichen Unfallfolgen zu begrenzen. Die Unfallvermeidung hat stets Vorrang vor dem Abmildern der Unfallfolgen. Beim Konzept *Defence-in-Depth* werden Technik und Prozeduren in verschiedenen Level hierarchisch eingesetzt. Dabei ist das Ziel, die Effektivität der physischen Barrieren zu erhalten, die zwischen den verwendeten radioaktiven Materialien und den Menschen stehen. Dabei werden sowohl technische Ausfälle als auch menschliche Fehler ausgeglichen. Auch Ereignisse, die ihren Ursprung außerhalb der Kernkraftanlage haben, werden in dem Konzept berücksichtigt.
Das Konzept *Defence-in-Depth* ist in fünf Level (level of protection) untergliedert (siehe auch Abbildung 2.3). Versagt ein Level, dann bieten die nachfolgenden Level noch Schutz. Die fünf Level nach [Int96] sind:

Level 1 Vermeidung von Systemausfällen und Unregelmäßigkeiten
Level 2 Erkennen von Systemausfällen und Beherrschung von Unregelmäßigkeiten
Level 3 Sicherstellen, dass Sicherheitsfunktionen dennoch weiterhin ausgeführt werden, indem spezielle Sicherheitssysteme aktiviert werden oder durch andere Sicherheitsmerkmale, die keiner Aktivierung bedürfen
Level 4 Unfallmanagement zum Begrenzen der Unfallverlaufs, um zu verhindern, dass radioaktives Material austritt, oder um die zu erwartenden schweren Unfallfolgen abzumildern

Level 5 Abmildern der radiologischen Auswirkungen, die durch das Austreten radioaktiver Substanzen entstehen, durch Notfallschutzmaßnahmen außerhalb der Kernkraftanlage

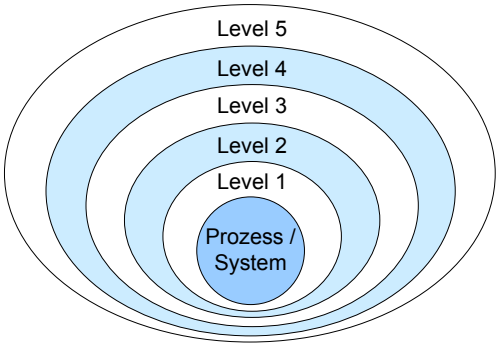

Abbildung 2.3: Die fünf Level des Konzepts *Defence-in-Depth*

2.3.3 Schutzebene

Schutzebene ist ein Begriff, der vor allem in der Prozessindustrie verwendet wird. Der ursprüngliche Begriff ist das englische *layer of protection*. Alternativ werden auch die Bezeichnungen *protection layer* und *line of defence* verwendet. In der vorliegenden Arbeit wird die deutsche Übersetzung *Schutzebene* nach Börcsök [Bö6] und der DIN EN 61511-1 [DIN05a] verwendet.
Laut DIN EN 61511-1 ist eine Schutzebene eine „unabhängige Maßnahme, die das Risiko durch Regelung oder Steuerung, Schutz- oder Schadensbegrenzungsmaßnahmen vermindert“ [DIN05a, 3.2.59]. In der chemischen Industrie, einem Teilgebiet der Prozessindustrie, ist der Begriff Schutzebene selbst nicht explizit definiert. Das Center for Chemical Process Safety (CCPS) definiert stattdessen in [Cen93] den wichtigen Begriff der *unabhängigen Schutzebene* (USE) (Independent Protection Layer (IPL)): Ein System, das speziell dafür entworfen wurde, die Wahrscheinlichkeit oder die Schwere der Auswirkungen eines identifizierten gefährlichen Ereignisses um einen großen Faktor zu reduzieren, d. h. durch eine Reduzierung der Wahrscheinlichkeit um mindestens das 100-fache. Eine USE muss unabhängig von anderen Schutzebenen sein (bezogen auf das gefährliche Ereignis), sowie verlässlich und auditierbar.
Diese Definition aus [Cen93] unterscheidet sich von der aus der DIN EN 61511-1 [DIN05a] dadurch, dass eine Schutzebene unabhängig sein kann oder nicht. Die Schutzebenen nach der DIN EN 61511-1 müssen unabhängig sein. Wie aus der Definition des CCPS [Cen93] ersichtlich ist, stellt die chemische Industrie darüber hinaus noch weitere Anforderungen an ihre Schutzebenen. Bemerkenswert ist hierbei vor allem die Forderung, dass eine Schutzebene das Risiko *beträchtlich* senken muss.

2.3.4 Sicherheitsfunktion

Gemäß der DIN EN 61508-4 [DIN11b] ist eine *Sicherheitsfunktion* (safety function) eine „Funktion, die von einem sicherheitsbezogenen E/E/PE-System oder anderen risikomindernden Maßnahmen ausgeführt wird, und dazu vorgesehen ist, unter Berücksichtigung eines festgelegten gefährlichen Vorfalls [...] einen sicheren Zustand für die EUC[7] zu erreichen oder aufrechtzuerhalten“ [DIN11b, 3.5.1]. Der Begriff Sicherheitsfunktion der DIN EN 61508-4 [DIN11b] ist rigoroser als z. B. der Begriff Schutzebene (siehe Abschnitt 2.3.3). Hier geht es nicht nur um die Reduktion des Risikos, sondern um das Erreichen eines sicheren Zustands. In solch einem sicheren Zustand ist das Risiko so klein, dass es ohne weitere Maßnahmen akzeptiert werden kann.

[7] Equipment Under Control (Anmerkung der Autorin)

Eine alternative, deutlich allgemeinere Definition für den Begriff Sicherheitsfunktion ist bei Harms-Ringdahl in [HR01] zu finden: Eine Sicherheitsfunktion ist eine technische, organisatorische oder kombinierte Funktion, die die Wahrscheinlichkeit und / oder die Folgen von Unfällen oder anderen unerwünschten Ereignissen in einem System verringern kann.

2.3.5 Sicherheitskritische Funktion

Der Begriff *sicherheitskritisch* wird in verschiedenen Domänen verwendet, in Bezug auf Funktionen, Systeme, Software und Ausfälle, häufig jedoch, ohne ihn genau zu definieren. Johnsen et al. [JHVR06] verwenden das Wort sicherheitskritisch in Bezug auf Funktionen bei Betrachtungen zum Thema Sicherheitskultur im grenzüberschreitenden Eisenbahnbetrieb. Sie definieren den Begriff *sicherheitskritische Funktion* als Funktion eines Systems, bei der eine Fehlfunktion sofort das Risiko von Verletzungen oder Gesundheitsschäden erhöhen würde [JHVR06].
Der Begriff sicherheitskritische Funktion ist deutlich allgemeiner als der Begriff Sicherheitsfunktion der DIN EN 61508-4 [DIN11b] (Abschnitt 2.3.4). Eine Sicherheitsfunktion ist zielgerichtet, bezieht sich auf ein bestimmtes Ereignis und soll einen sicheren Zustand herbeiführen bzw. beibehalten. Eine sicherheitskritische Funktion wirkt allgemein risikomindernd (oder im Fall einer Fehlfunktion risikoerhöhend) und ist unabhängig vom Erreichen (oder Vorhandensein) eines sicheren Zustands.

2.3.6 Sicherheitsbezogenes System

Unter einem *sicherheitsbezogenen System* (safety-related system) versteht die DIN EN 61508-4 [DIN11b] ein System, das „sowohl die erforderlichen Sicherheitsfunktionen ausführt, die notwendig sind, um einen sicheren Zustand für die EUC zu erreichen oder aufrechtzuerhalten, als auch dazu vorgesehen ist, selbst oder mit anderen sicherheitsbezogenen E/E/PE-Systemen und anderen risikomindernden Maßnahmen die notwendige Sicherheitsintegrität für die geforderten Sicherheitsfunktionen zu erreichen“ [DIN11b, 3.4.1]. Ein sicherheitsbezogenes System dient dazu, (ggf. zusammen mit anderen Maßnahmen) das Risiko, das von Gefährdungen ausgeht, auf ein tolerierbares Risiko zu senken [DIN11b].
Anmerkung: DIN EN 61508-4 unterscheidet explizit zwischen dem Equipment Under Control (EUC) und dem sicherheitsbezogenem System. Die Norm geht davon aus, dass ein sicherheitsbezogenes System dem eigentlichen System hinzugefügt werden muss. Mit dieser Trennung unterscheidet sich diese Definition von den meisten anderen Definitionen, bei denen Sicherheitsfunktion und betriebliche Funktion von ein und demselben System ausgeführt werden können.

2.3.7 Fazit

Die oben aufgeführten Begriffe aus unterschiedlichen Domänen bilden eine Auswahl von Begriffen aus dem Umfeld der Sicherheitsschichten. Sie haben jeweils leicht unterschiedliche Bedeutungen (Begriffsinhalte) und sind auf ihren jeweiligen Anwendungsbereich zugeschnitten. Der Kerngedanke ist jedoch stets gleich. Alle vorgestellten Begriffe dienen der Risikoreduktion, der Aufrechterhaltung der Sicherheit und dem Schutz von Menschen vor Schaden. Eine Vereinheitlichung und / oder Integration der Begriffe wäre hilfreich, um Energien zu bündeln und interdisziplinäres, domänenübergreifendes Arbeiten sowie die Übertragbarkeit der Konzepte von einer Domäne in eine andere zu erleichtern. Dies ist jedoch nicht Gegenstand der vorliegenden Arbeit.
Gegen eine Vereinheitlichung der Begriffe spricht die Tatsache, dass jede Domäne spezielle Randbedingungen und Anforderungen besitzt, sodass ein vereinheitlichter Begriff im Einzelfall zu einschränkend oder aber zu unspezifisch sein kann. Aus diesem Grund und auch aus Gründen der Tradition und Gewohnheit werden zweifelsohne verschiedene Begriffe nebeneinander bestehen bleiben.

Aus diesen Gründen wird für die in den Abschnitten 2.3.1 bis 2.3.6 aufgeführten Begriffe auf die Erstellung eines strukturierten Begriffssystems, wie dies z. B. bei Drewes [Dre09] für den Begriff Sicherheit geschehen ist, verzichtet. Stattdessen werden die Begriffe mit Hinblick auf das Teilziel der vorliegenden Arbeit, die Definition des Begriffs *Sicherheitsschicht*, bewertet. Sie werden daraufhin untersucht, ob einer von ihnen der Idee einer Sicherheitsschicht, wie sie in [PSM07] und [SP07] formuliert wurde, nahe kommt.
Das *sicherheitsbezogene System* (Abschnitt 2.3.6) entstammt dem Umfeld der E/E/PE-Systeme und umfasst daher weder Prozeduren noch Personen, die jedoch Teil einer Sicherheitsschicht sein können. Die rein funktionalen Begriffe *sicherheitskritische Funktion* (Abschnitt 2.3.5) und *Sicherheitsfunktion* (Abschnitt 2.3.4) sind nicht ausreichend, um die Idee einer Sicherheitsschicht zu beschreiben, da Sicherheitsschichten auch Technik und Komponenten enthalten. *Schutzebene* (Abschnitt 2.3.3) ist ein Begriff, der selbst nicht klar definiert ist. Der stattdessen definierte Begriff der unabhängigen Schutzebene (USE), verlangt, dass ein System die Wahrscheinlichkeit eines gefährlichen Ereignisses um mindestens das 100-fache reduzieren muss, um als USE zu gelten. Eine solche Forderung wurde für Sicherheitsschichten bisher nicht aufgestellt und ist auch nicht sinnvoll, da auch kleine Beiträge zur Sicherheit nutzbringend sind. Das Konzept der *Defence-in-Depth* (Abschnitt 2.3.2) ist durch die Untergliederung in fünf Level bereits zu stark festgelegt, als dass es für die Idee einer Sicherheitsschicht geeignet wäre.
Der Begriff *Sicherheitsbarriere* (Abschnitt 2.3.1) hingegen ist weit genug gefasst, um alle Aspekte der Idee einer Sicherheitsschicht zu umfassen. Er ist weit verbreitet und wird in verschiedenen Domänen benutzt. Allerdings umfasst der Begriff der Barriere sehr viel und wird entsprechend flexibel benutzt. Sklet selbst bemerkt, dass beinahe alles als Barriere betrachtet werden kann [Skl06]. Sicherheitsschichten hingegen sollen kombinierbar und austauschbar sein [PSM07]. Daraus ergibt sich die Forderung nach einer ausreichenden Unabhängigkeit der Sicherheitsschichten voneinander. Ohne eine solche Unabhängigkeit würde das Austauschen einer Sicherheitsschicht gegen eine andere möglicherweise die Wirksamkeit der anderen Sicherheitsschichten beeinträchtigen. An Barrieren sind keinerlei Unabhängigkeitsanforderungen gestellt. Daher kann auch der Begriff der (Sicherheits-)Barriere die Idee einer Sicherheitsschicht nicht vollständig beschreiben. Der Begriff Sicherheitsschicht muss neu definiert werden.

3 Sicherheitsschichten

3.1 Anforderungen an Sicherheitsschichten

Der Begriff *Sicherheitsschicht* soll eine Kombination aus Technik und Prozeduren, Komponenten, Regeln und Personen bezeichnen, deren Zweck es ist, Risiken zu mindern, Gefahren abzuwenden und Unfälle zu verhindern (siehe Abschnitt 2.3). Der Begriff wurde bereits im Eisenbahnbereich verwendet [SP07], ohne jedoch klar definiert worden zu sein. Wie in Abschnitt 2.3 dargestellt, gibt es in der Literatur zahlreiche Begriffe, die der Idee einer Sicherheitsschicht nahe kommen. Jedoch eignet sich keiner, um diese Idee vollständig zu beschreiben (siehe Abschnitt 2.3.7). Daher soll im Folgenden eine Definition des Inhalts des Begriffs Sicherheitsschicht erarbeitet werden. Zuvor werden jedoch die recht vagen Anforderungen aus [PSM07, SP07] an den Begriff Sicherheitsschicht konkretisiert.

- S-1 Sicherheitsschichten sollen Bausteine in einem Baukasten sein, um ein Portfolio bilden zu können, wie in [SP07] gefordert.
- S-2 Sicherheitsschichten sollen einen modularen und flexiblen Aufbau von Sicherheitssystemen ermöglichen, wie in [PSM07] gefordert.
- S-3 Sicherheitsschichten sollen für Sicherheitsnachweise verwendet werden können, damit die Kenntnis der Sicherheitsschichten eines Systems auch Vorteile bei der Zulassung mit sich bringt.
- S-4 Sicherheitsschichten sollen Raum für Innovationen und andere Lösungen geben, um eine beständige Weiterentwicklung der Sicherheitssysteme zu ermöglichen und Kosten zu sparen.
- S-5 Der Begriff Sicherheitsschicht soll klar definiert sein.
- S-6 Der Begriff Sicherheitsschicht soll funktionale Aspekte umfassen, um den funktionalen Ansatz der CENELEC-Normen zu berücksichtigen.
- S-7 Der Begriff Sicherheitsschicht soll technische Aspekte umfassen. Systementwickler aus dem Eisenbahnbereich denken bevorzugt in Form von technischen Komponenten. Eine rein funktionale Betrachtungsweise von Sicherheitsschichten wäre daher nicht ausreichend. Außerdem ist es die Technik, die letztendlich gebaut und zugelassen werden soll.
- S-8 Der Begriff Sicherheitsschicht soll Organisatorisches, wie z. B. Regeln, und Menschen umfassen. Es wird ein ganzheitlicher Ansatz benötigt. Dies wird auch von den CENELEC-Normen gefordert.
- S-9 Sicherheitsschichten sollen so gestaltet sein, dass das Entfernen einer Sicherheitsschicht die anderen noch verbleibenden Sicherheitsschichten nicht beeinflusst.
- S-10 Sicherheitsschichten sollen so gestaltet sein, dass eine Sicherheitsschicht gegen eine andere ausgetauscht werden kann, ohne dass das Gesamtsystem einer komplett neuen, aufwändigen Bewertung unterzogen werden muss.
- S-11 Der Begriff Sicherheitsschicht soll Aspekte zur Unabhängigkeit enthalten. Unabhängigkeit ist beim Erreichen einer angemessenen Sicherheit im Eisenbahnbereich ein bedeutendes Prinzip. Jeder Sicherheitsnachweis muss Auskunft über die Unabhängigkeit der Einheiten des Systems geben.

S-12 Der Begriff Sicherheitsschicht soll auf Gefährdungen bezogen sein. Dies harmoniert mit dem Ansatz der CENELEC-Normen, bei denen Maßnahmen zur Risikominderung im Hinblick auf Gefährdungen definiert und dokumentiert werden, u. a. im sogenannten Gefahrenprotokoll (Hazard Log), siehe [DIN00].

Folgende Anforderungen bestehen explizit nicht:

S-13 Eine Sicherheitsschicht braucht keine Mindestanforderungen bezüglich der Risikoreduktion zu erfüllen. Sie muss das Risiko nicht um einen bestimmten Mindestfaktor reduzieren (im Gegensatz zu anderen Konzepten, vergleiche Abschnitt 2.3.3). Kleine Beiträge zur Sicherheit sind ebenfalls nutzbringend.

S-14 Ein Modell der Sicherheitsschichten braucht keine festgelegte Reihenfolge zu beinhalten (im Gegensatz zu anderen Konzepten, vergleiche z. B. Abschnitt 4.3). Es ist unwichtig, in welcher Reihenfolge Sicherheitsschichten wirken, solange sie der Sicherheit des Systems dienen.

3.2 Definition des Begriffs Sicherheitsschicht

In diesem Abschnitt werden, unter Berücksichtigung der Anforderungen S-1 bis S-14, der Begriff Sicherheitsschicht sowie alle dafür notwendigen Teilbegriffe definiert. Damit wird der Begriffsinhalt festgelegt und somit die bisherige Lücke in der Literatur gefüllt (siehe Abschnitt 2.3).

3.2.1 Sicherheitsschicht

Eine Sicherheitsschicht (SiS) ist ein unabhängiges Barriere-Funktions-Paar (B-F-Paar), das prinzipiell in der Lage ist, das Eintreten eines bestimmten unerwünschten Ereignisses bzw. einer Gefährdung zu verhindern (siehe Abbildung 3.1).

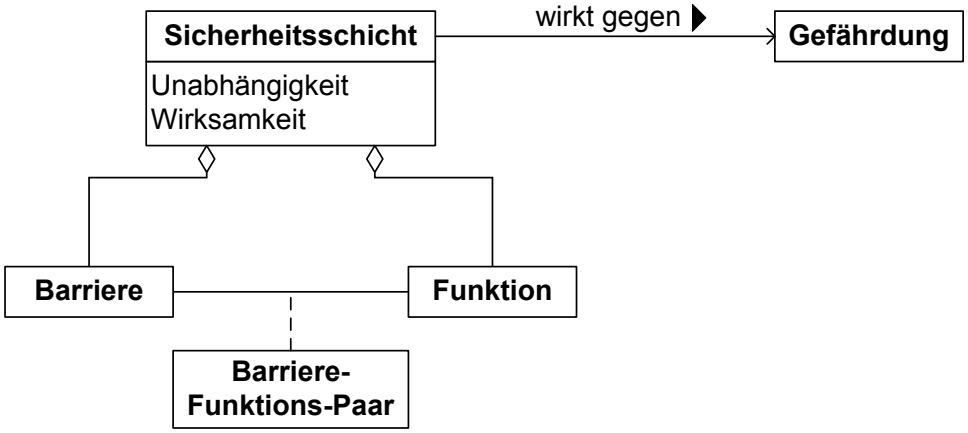

Abbildung 3.1: Der Begriff Sicherheitsschicht als Klassendiagramm

Eine Sicherheitsschicht besteht aus einer Barriere und einer Funktion, die zusammen ein Barriere-Funktions-Paar bilden. Eine Sicherheitsschicht besitzt die Merkmale Unabhängigkeit und Wirksamkeit und wirkt gegen eine oder auch mehrere Gefährdungen. Die Begriffe Barriere, Funktion, Wirksamkeit und Unabhängigkeit werden im Folgenden definiert.

3.2.2 (Sicherheits-)Barriere

Wie in Abschnitt 2.3.1 erläutert, wird in der vorliegenden Arbeit für den Begriff Sicherheitsbarriere die Definition von Sklet verwendet und die Benennung Barriere als Kurzform für Sicherheitsbarriere verwendet:
Eine **(Sicherheits-)Barriere** ist ein physisches und / oder nicht-physisches Mittel, das geplant wurde, um unerwünschte Ereignisse oder Unfälle zu vermeiden, zu beherrschen oder abzumildern [Skl06].
Barrieren sind Gegenstände, Regeln, organisatorische Maßnahmen etc., die der obigen Definition genügen. Im Rahmen der vorliegenden Arbeit soll der Begriff Barriere für Klassen von Mitteln (z. B. Überwachungssignale oder andere Signale) verwendet werden. Sehr konkrete Gegenstände, z. B. das Überwachungssignal der Firma XYZ bei Streckenkilometer 82,6, wird als *Barrieresystem* bezeichnet. Das Attribut „geplant“ bedeutet, dass mindestens ein Zweck der Barriere darin besteht, das Risiko eines unerwünschten Ereignisses zu reduzieren (siehe Abschnitt 2.3.1). Der Aspekt der Planung soll jedoch nicht so stark gefasst werden, dass eine wirksame Barriere, die gegen eine Gefahr schützt, nur deshalb nicht als Barriere bezeichnet wird, weil sie eigentlich zu einem ganz anderen Zweck geplant wurde. Wichtig ist nicht die ursprüngliche Absicht, die zu der Entwicklung der Barriere geführt hat, sondern ihr derzeitiger Zweck. Dieser Zweck muss sich auf eine Risikoreduktion beziehen und er muss auch *bekannt* sein, denn nur dadurch wird sichergestellt, dass die Barriere nicht unbedachterweise entfernt wird und dadurch eine Sicherheitslücke entsteht.

3.2.3 (Sicherheitsbarriere-)Funktion

Im Zusammenhang mit Sicherheitsschichten soll unter dem Begriff *Funktion* die Funktion der Barriere (siehe Abschnitt 3.2.2), also die Sicherheitsbarrierefunktion verstanden werden. Da für den Begriff Barriere die Definition von Sklet verwendet wurde, soll auch für den Begriff Funktion Sklets Definition verwendet werden:
Eine **(Sicherheitsbarriere-)Funktion** ist nach Sklet [Skl06] eine Funktion, die geplant wurde, um unerwünschte Ereignisse oder Unfälle zu vermeiden, zu beherrschen oder abzumildern. Eine Funktion sollte immer mit eine Verb und einem Nomen beschrieben werden, z. B. „Geschwindigkeit reduzieren“. Die Funktion beschreibt den Zweck der Barriere. Eine Barriere kann mehrere Funktionen haben. Zu einem Barriere-Funktions-Paar (B-F-Paar) gehören jedoch immer genau eine Barriere und eine Funktion.

3.2.4 Wirksamkeit

Eine Sicherheitsschicht muss gegen das unerwünschte Ereignis *wirksam* sein. Das bedeutet, ein Barriere-Funktions-Paar ist eine SiS mit Hinblick auf ein unerwünschtes Ereignis / eine bestimmte Gefährdung. Eine SiS ist also stets zielgerichtet. Des Weiteren muss eine SiS die Eigenschaft haben, das Eintreten des unerwünschten Ereignisses allein verhindern zu können – zumindest in bestimmten Situationen. Kann ein B-F-Paar das nicht, ist es keine vollständige SiS. Es kann dennoch bedeutsam für die Sicherheit sein, z. B. als Bestandteil einer SiS oder als notwendige Voraussetzung für das Wirken einer SiS.

3.2.5 Unabhängigkeit

Unabhängigkeit ist im Bereich der Sicherheit eine wichtige Eigenschaft. Unabhängigkeit ist erwünscht, denn sie verteilt die Sicherheitsverantwortung auf verschiedene (Teil-)Systeme, sodass ein einzelner Ausfall die Sicherheit des Systems nicht beeinträchtigen kann. Daher sind Forderungen zur Unabhängigkeit oft Gegenstand von Normen wie z. B. der DIN EN 50129 [DIN03], die vorschreibt,

dass das Thema „Unabhängigkeit von Betrachtungseinheiten“ in jedem Sicherheitsnachweis behandelt werden muss. Unabhängigkeit ermöglicht es zudem, bei der Berechnung der Eintretenswahrscheinlichkeiten von unerwünschten Ereignissen einfache mathematische Formeln zu verwenden, die auch per Hand ausgewertet werden können.
Unabhängigkeit in der Realität hat mit der Sicherheit etwas gemeinsam: So wie es nie 100%ige Sicherheit gibt, so gibt es auch nie 100%ige Unabhängigkeit. Ein System ist sicher, wenn das verbleibende Restrisiko tolerierbar ist. Dem entsprechend ist eine Einheit unabhängig, wenn der verbleibende Grad an Abhängigkeit so gering ist, dass er (insbesondere stochastisch) nicht mehr ins Gewicht fällt.

Ziel der Unabhängigkeit von Sicherheitsschichten

Neben den zuvor genannten generellen Vorteilen und Zielen, soll die Unabhängigkeit von Sicherheitsschichten eine ausreichende Modularität der Sicherheitsschichten sicherstellen. Durch diese Modularität kann ein Portfolio von Sicherheitsschichten gebildet werden, das als Grundlage für den Austausch von Sicherheitsschichten im Zuge der Veränderung eines Systems dient.
Insbesondere soll die Unabhängigkeit zwischen Sicherheitsschichten sicherstellen, dass

1. der Ausfall einer SiS nicht zum Ausfall einer anderen SiS führt (Domino-Effekt)
2. eine SiS aus dem System entfernt werden kann, ohne dass andere SiS dadurch beschädigt werden.

Anforderungen an die Unabhängigkeit von Sicherheitsschichten

Aus diesen beiden Zielen leiten sich weitere Forderungen an die Unabhängigkeit von Sicherheitsschichten ab:

- Die Funktion einer SiS darf nicht Teilfunktion einer Funktion einer anderen SiS sein.
- Es darf nicht die Funktion einer SiS sein, eine andere SiS zu aktivieren oder zu deaktivieren.
- Eine SiS darf nicht Teil einer anderen SiS sein.
- Die Barriere einer SiS darf nicht Teil einer Barriere einer anderen SiS sein.
- Die Barriere einer SiS darf kein technisches Betriebsmittel gemeinsam mit einer Barriere einer anderen SiS benutzen.
- Eine Barriere einer SiS darf nicht in der Lage sein, durch eine Fehlfunktion eine Barriere einer anderen SiS zu deaktivieren oder in einer anderen Weise in ihrer Wirksamkeit zu beeinträchtigen.

Unabhängigkeitskriterien

Damit gelten die folgenden Kriterien für die Unabhängigkeit von Sicherheitsschichten: Ein B-F-Paar ist unabhängig von allen anderen B-F-Paaren des betrachteten Systems (im Hinblick auf die betrachtete Gefährdung), wenn gilt:

a) Die Funktion des B-F-Paars ist keine (echte) Teilfunktion eines anderen B-F-Paars.
b) Die Barriere des B-F-Paars ist kein Teil einer Barriere eines anderen B-F-Paars.
c) Es ist nicht die Funktion des B-F-Paars, ein anderes B-F-Paar zu aktivieren oder zu deaktivieren.
d) Die Barriere des B-F-Paars ist nicht in der Lage, durch eine Fehlfunktion oder einen Ausfall eine Barriere eines anderen B-F-Paars zu deaktivieren oder in einer anderen Weise in ihrer Wirksamkeit zu beeinträchtigen.
e) Die Barriere des B-F-Paars teilt kein technisches Betriebsmittel mit einer Barriere eines anderen B-F-Paars.

Achtung: Punkt **a**) bedeutet nicht, dass zwei unabhängige B-F-Paare nicht die gleiche Funktion ausüben können. Hat ein B-F-Paar die gleiche Funktion wie ein anderes B-F-Paar, dann ist dies keine

echte Teilfunktion. Kriterium **a**) bedeutet lediglich, dass kein B-F-Paar darauf angewiesen ist, dass ein anderes B-F-Paar funktioniert.

3.2.6 Grenzen der Unabhängigkeit

Bei der Frage nach der Unabhängigkeit von Sicherheitsschichten sind die Systemgrenzen von besonderer Bedeutung. Das „System“ Sicherheitsschicht darf nicht größer definiert werden als unbedingt notwendig. Abbildung 3.2 zeigt hierzu ein Beispiel: Zwei verschiedene Sicherheitsschichten A und B eines Eisenbahnsystems benötigen Strom, um zu funktionieren. Wird die Systemgrenze der Sicherheitsschichten so weit gefasst, dass sie die Stromquelle (z. B. das Elektrizitätswerk) mit umfasst, dann sind beide SiS nicht mehr unabhängig voneinander. Der Ausfall des Elektrizitätswerks ist ein Ausfall der SiS A und B, da die Stromquelle als Teil der SiS betrachtet wurde. In diesem Fall hätte ein Ausfall von SiS A (Komponente Elektrizitätswerk) auch einen Ausfall von SiS B zur Folge.

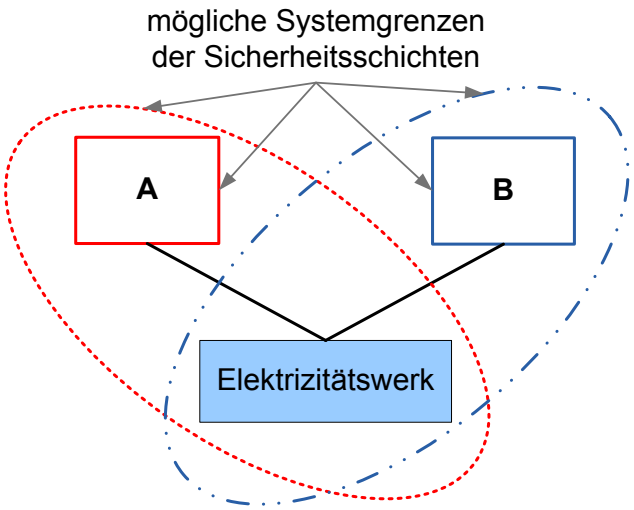

Abbildung 3.2: Bedeutung der Systemgrenzen von Sicherheitsschichten für die Unabhängigkeit

Der Ausfall des Elektrizitätswerks führt zum Ausfall beider SiS. Dies ist jedoch nicht die Form von Abhängigkeit, die im Rahmen des Modells der Sicherheitsschichten relevant ist. Wie bereits oben bemerkt, gibt es in der Realität fast nie 100%ige Unabhängigkeit. Alles ist mit allem verbunden, sagt ein Sprichwort. Doch auch wenn die SiS A und B durch einen Stromausfall beide nicht mehr funktionieren, können sie doch eine gewisse Unabhängigkeit besitzen, eine Unabhängigkeit, die für die Sicherheit des betrachteten Systems von Bedeutung ist.
Es ist die Aufgabe von Analysen von Ausfällen aufgrund einer gemeinsamen Ursache (Common Cause Failure Analysis (CCFA)), Fälle aufzudecken, in denen eine Ursache zu mehreren Ausfällen im System führen kann, und somit abhängige Einheiten zu identifizieren. Sind zwei Einheiten nicht voneinander unabhängig, dann müssen die identifizierten Common Cause Failures (CCF) bei den Sicherheitsbetrachtungen berücksichtigt werden. Insbesondere bei quantitativen Analysen ist dies schwierig, da geeignete Daten für das Auftreten von CCF schwer zu bekommen sind. Werden als Alternative geeignete Abschätzungen zu getroffen, besteht die Schwierigkeit darin, diese als glaubwürdig zu argumentieren. Daher ist Unabhängigkeit ein großer Vorteil. Allerdings ist völlige Unabhängigkeit aufgrund der fortschreitenden technologischen Entwicklung (zunehmender Einsatz von Computern, Speicherprogrammierbaren Steuerungen, Datennetzen etc.) immer schwieriger zu erreichen.
Da viele Barrieren Strom benötigen und in der Regel keine eigenständige, vollständig getrennte Stromquelle besitzen, ist ein gewisses Maß an Abhängigkeit unvermeidbar. Diese Art Abhängigkeit kann für den Zweck der vorliegenden Arbeit jedoch vernachlässigt werden. Entsprechendes gilt für ähnliche Gemeinsamkeiten von Barrieren, z. B. Ort (im gleichen Gebäude, auf gleicher Höhe), Infor-

mationsquelle (Stellwerk) etc. Beachtet werden müssen hingegen Abhängigkeiten zwischen Barrieren, die durch gemeinsam genutzte technische Betriebsmittel entstehen, wie z. B. denselben Prozessor in einem Computer oder ein Relais, das durch zwei Kontakte zwei Einheiten steuert. Diese Abhängigkeiten führen dazu, dass diese Barrieren nicht Bestandteil verschiedener SiS sein können.

3.2.7 Besonderheit: Der Mensch als Teil einer Sicherheitsschicht

Eine Besonderheit bzgl. der Unabhängigkeit sind Sicherheitsschichten, bei deren Wirken der Mensch eine Rolle spielt. Bei technischen Systemen wird klassischerweise davon ausgegangen, dass Ausfälle auf ein Versagen der Hardware zurückzuführen sind (z. B. auf das Verschweißen eines Relais-Kontakts). Ein solcher Fehler ist permanent, d. h. das System kann seine Funktion von nun an nicht mehr wahrnehmen, solange bis es repariert wurde. In vielen Sicherheitsbetrachtungen wird vereinfacht angenommen, dass ein technisches System mit einem Ausfall insgesamt defekt ist (Totalausfall) und keine seiner Funktionen mehr korrekt ausführen kann[1]. Wenn also ein technisches System zwei Funktionen von zwei unterschiedlichen SiS implementiert, dann bedeutet ein solcher Ausfall das Ende der Funktionsfähigkeit beider SiS. Daher die Forderung nach technischer Unabhängigkeit, d. h. keine gemeinsamen technischen Betriebsmittel.

Der Mensch hingegen kann mehrere Funktionen ausüben und dabei Teil mehrerer unabhängiger SiS sein. Denn im Gegensatz zu einem technischen System bedeutet bei einem Menschen ein Fehler nicht gleich einen „Totalausfall“ des Systems (des Menschen). Solche „Totalausfälle“ gibt es natürlich auch beim Menschen, er kann z. B. während der Arbeit einschlafen, wodurch er seine Aufgaben nicht mehr wahrnehmen kann. Die Sicherheitsfahrschaltung (Sifa) ist ein klassisches System, das im Falle eines „Totalausfalls“ eines Triebfahrzeugführers eingreifen und den Zug zum Stillstand bringen soll. Viel häufiger beim Menschen sind hingegen ein Irrtum, ein Vergessen einer Handlung, eine Fehleinschätzung der Situation oder eine fehlerhafte Ausführung der Aufgabe. Hierbei muss ein Fehler nicht zwangsläufig einen weiteren zur Folge haben. Dies gilt insbesondere dann, wenn die Aufgaben des Menschen unterschiedlich sind, er also unterschiedliche Funktionen übernimmt. Beispielsweise kann ein Triebfahrzeugführer (Tf) vergessen, vor einem unbeschrankten Bahnübergang (BÜ) ein akustisches Signal zu geben. Aber aus diesem Fehler kann nicht geschlossen werden, dass er auch am nächsten Halt zeigenden Signal vorbeifährt. Es ist nicht einmal zwingend, dass der Tf das akustische Signal am nächsten BÜ ebenfalls vergisst. Der Mensch kann verschiedene Fehler unabhängig voneinander machen, seinen Fehler selbst erkennen und möglicherweise sogar noch korrigieren. Daher müssen die Unabhängigkeitskriterien für SiS beim Menschen nicht so streng ausgelegt werden, d. h. die Kriterien **b**) und **d**) sind für den Menschen in der Regel nicht anwendbar. Das gilt allerdings nur, solange der Mensch nicht komplett aus einem System entfernt wird (Stichwort vollautomatischer Betrieb, z. B. fahrerlose U-Bahn). Ein Entfernen des Menschen aus dem System entfernt natürlich alle SiS, an denen er beteiligt ist. Hingegen ist es durchaus möglich, eine einzelne SiS, an der der Mensch beteiligt ist, zu entfernen, ohne die anderen SiS zu entfernen.

Bei Barrieren, die zur Umsetzung einen Menschen benötigen, wird eine sprachliche Vereinfachung verwendet. Typische Beispiele sind Signale und Schilder. Ohne den Menschen sind sie wirkungslos. Wenn also ein Schild als Barriere bezeichnet wird, dann steht dahinter immer die Teilnahme des Menschen. Der Einfachheit halber wird eine solche Barriere als Schild bezeichnet statt als „Schild, dessen Inhalt vom Menschen befolgt wird“.

[1] In der Realität kann es vorkommen, dass ein System mit einem defekten Bauteil durchaus noch Teile seiner Funktion erfüllen kann, zumindest unter besonderen, günstigen Bedingungen. Allerdings ist dies unsicher und schwer zu modellieren, sodass man sich bei Sicherheitsbetrachtungen nicht darauf stützt und stattdessen Worst-Case-Annahmen trifft.

3.3 Vergleich mit anderen Definitionen

Zur Einordnung des Begriffs Sicherheitsschicht in die bestehende Begriffswelt, zur Reflexion und zur Verdeutlichung der Unterschiede zu anderen Definitionen wird im Folgenden die Definition des Begriffs Sicherheitsschicht mit anderen Definitionen verglichen. Dazu wird zunächst der Aspekt der Unabhängigkeit betrachtet. Anschließend erfolgt ein Vergleich mit Begriffen, die dem der Sicherheitsschicht ähneln.

3.3.1 Vergleich mit anderen Definitionen von Unabhängigkeit

Im Eisenbahnbereich sind die CENELEC-Normen von großer Bedeutung. In ihnen, genauer gesagt in der DIN EN 50129 [DIN03] gibt es ebenfalls Definitionen von Unabhängigkeit. Die DIN EN 50129 unterscheidet zwischen funktionaler und physikalischer Unabhängigkeit.

Funktionale Unabhängigkeit wird in der Norm definiert als das „Freisein von allen Mechanismen, die den korrekten Ablauf von mehr als einer Funktion auf Grund von systematischen oder zufälligen Fehlern beeinträchtigen können“ [DIN03, 3.1.26]. Die funktionale Unabhängigkeit spielt in der Norm eine Rolle bei der Aufteilung der tolerierbaren Gefährdungsrate (THR) auf Funktionen und Teilsysteme. Sie ist eine wünschenswerte Eigenschaft, denn sie vereinfacht den Prozess der Aufteilung der THR. Allerdings merkt die DIN EN 50129 [DIN03] selbst an, dass Funktionen im Allgemeinen nicht unabhängig sind.

Die Definition der funktionalen Unabhängigkeit ist den Unabhängigkeitskriterien für SiS aus Abschnitt 3.2.5 ähnlich, allerdings unspezifischer formuliert, d. h. es gibt keine konkreten Kriterien, mit denen die Unabhängigkeit geprüft werden kann. Die Definition ist darüber hinaus sehr streng, was dazu führt, dass es kaum Funktionen gibt, die dem Unabhängigkeitsbegriff der Norm genügen. In der DIN EN 50129 steht dazu folgende Anmerkung: „Es ist zu beachten, dass im Allgemeinen Funktionen nicht unabhängig sind.“ [DIN03]. D. h. die DIN EN 50129 definiert eine Art von Unabhängigkeit, die in der Realität so im Allgemeinen nicht zu finden sein wird. Die funktionale Unabhängigkeit der Norm bedeutet Freisein von Fehlern mit gemeinsamer Ursache (CCF). CCF gibt es in der Realität (fast) immer, sei es System-intern oder -extern. Doch trotz dieser CCF ist Unabhängigkeit ein wichtiges Thema, denn auch eine teilweise Unabhängigkeit verbessert die Sicherheit durchaus. CCF müssen allerdings zusätzlich betrachtet werden. Die DIN EN 50129 merkt dazu an: Funktionen „können aber in unabhängige Teilfunktionen und Teilfunktionen, die durch gemeinsam wirkende Fehler (CCF) abhängig sind, aufgeteilt werden“ [DIN03]. Diese Vorgehensweise kann auch auf die Funktionen der Sicherheitsschichten angewandt werden.

Die DIN EN 50129 definiert noch eine weitere Form der Unabhängigkeit: die physikalische Unabhängigkeit. **Physikalische Unabhängigkeit** ist das „Freisein von allen Mechanismen, die das korrekte Arbeiten von mehr als einem/r System / Teilsystem / Einrichtung auf Grund von zufälligen Fehlern beeinträchtigen können“ [DIN03, 3.1.28]. Diese Form der Unabhängigkeit konzentriert sich – im Gegensatz zur funktionalen Unabhängigkeit – auf die technische Umsetzung von Funktionen. Physikalische Unabhängigkeit spielt eine bedeutende Rolle bei der Erstellung und quantitativen Auswertung von Fehlerbäumen. Nur wenn zwei Einheiten physikalisch (und stochastisch, siehe unten) unabhängig sind, können sie im Fehlerbaum durch ein UND-Gatter verbunden werden. Der Einsatz von UND-verknüpften Einheiten kann die Ausfallrate eines Systems beträchtlich senken.

Diese Unabhängigkeit technischer Einheiten findet sich bei den Sicherheitsschichten in den Unabhängigkeitskriterien **b**), **d**) und **e**). Technische Einheiten eines Systems, die keine Sicherheitsschichten sind (z. B. eine (externe) gemeinsame Energieversorgung), werden durch diese Kriterien nicht erfasst. Daher ist eine CCF-Analyse stets notwendig.

Neben den beiden genannten Definitionen aus der DIN EN 50129 gibt es noch weitere Arten von Unabhängigkeit. Von besonderer Bedeutung ist der mathematische Begriff der **stochastischen Unabhängigkeit**. In der Stochastik sind zwei Ereignisse A und B aus der σ-Algebra $\mathfrak{A}$ eines Wahr-

scheinlichkeitsraumes (Ω, $\mathfrak{A}$, P) stochastisch unabhängig, wenn gilt: $P(A \frown B) = P(A) \cdot P(B)$. „Gilt $P(B) > 0$, so ist die Unabhängigkeit von A und B äquivalent zu $P(A|B) = P(A)$, d. h. die Wahrscheinlichkeit für das Eintreten von A wird nicht durch das Eintreten von B beeinflusst." [Wal02]. Im Gegensatz zur physikalischen Unabhängigkeit bezieht sich die stochastische Unabhängigkeit nicht auf Gegenstände, sondern auf Ereignisse, also z. B. auf den Ausfall einer Komponente oder das Entfernen einer Sicherheitsschicht. Ist A das Ereignis „Erfolgreicher Einsatz der Sicherheitsschicht a" und B das Ereignis „Entfernen der Sicherheitsschicht b", dann entspricht die stochastische Unabhängigkeit dem, was in Punkt 2 in Abschnitt 3.2.5 gefordert wird: Das Entfernen einer SiS darf die verbleibenden SiS nicht beeinflussen. Betrachtet man statt des Entfernens einer SiS den Ausfall einer SiS, so entspricht die stochastische Unabhängigkeit dem Punkt 1 aus Abschnitt 3.2.5. Das Unabhängigkeitskriterium **d**) stellt bzgl. der Ausfälle von Sicherheitsschichten die stochastische Unabhängigkeit sicher.

3.3.2 Vergleich mit anderen Begriffen

(Sicherheits-)Barriere (siehe Abschnitt 3.2.2) ist der wohl am weitesten verbreitete und am häufigsten genutzte Begriff, um Maßnahmen zu beschreiben, die verhindern, dass aus einer gefährlichen Situation ein Unfall entsteht. Der Begriff Sicherheitsschicht beinhaltet den Begriff der (Sicherheits-) Barriere und fügt noch die Funktion hinzu. Jede SiS beinhaltet eine Barriere. Allerdings ist nicht jede Barriere eine Sicherheitsschicht. Auch die Kriterien der Wirksamkeit und der Unabhängigkeit müssen erfüllt sein. Im allgemein üblichen Sprachgebrauch werden an eine Barriere keine so strengen Kriterien angelegt. Beinahe alles kann als Barriere gelten. Bei einer Sicherheitsschicht ist das anders.
Eine **USE** (Abschnitt 2.3.3) scheint bei oberflächlicher Betrachtung einer Sicherheitsschicht sehr ähnlich zu sein. Jedoch hat eine USE eine Eigenschaft, die für eine Sicherheitsschicht nicht gefordert ist: Eine USE muss das Risiko beträchtlich senken (mindestens um den Faktor 100) [Cen93]. Weniger effektive Maßnahmen dürfen also nicht die Bezeichnung USE tragen. Bei einer Sicherheitsschicht besteht keine derartige „Leistungsanforderung". Zudem erzwingt die Forderung nach einem Risikoreduktionsfaktor von mindestens 100 eine quantitative Analyse, wohingegen Sicherheitsschichten auch rein qualitativ betrachtet werden können. Gemäß der Definition von Börcsök [B06] muss eine USE das Risiko für das Auftreten eines bestimmten gefährlichen Ereignisses sogar auf ein *minimales* Restrisiko reduzieren. Der Begriff des minimalen Restrisikos birgt implizit eine Akzeptanz des verbleibenden Risikos. Das Restrisiko ist minimal, es kann nicht durch andere Maßnahmen noch weiter reduziert werden, daher muss es in Kauf genommen werden. Bei Sicherheitsschichten besteht keine Forderung nach einer Reduktion des Restrisikos auf ein Minimum. Eine solche Forderung würde der Idee von hintereinander gestaffelten Sicherheitsschichten zuwider laufen.
USE müssen, wie auch Sicherheitsschichten, bestimmten Unabhängigkeitskriterien genügen (siehe [Cen01]): USE müssen unabhängig vom Auftreten des auslösenden Ereignisses sein. USE müssen unabhängig von den Ausfällen aller anderen USE sein, die für eine bestimmtes Szenario[2] herangezogen werden. Insbesondere gilt, dass Schutzebenen, die durch einen Fehler mit gemeinsamer Ursache (CCF) ausfallen können, nicht als unabhängig gelten. Dies gilt auch, wenn der Fehler, der zum Ausfall führt, außerhalb der Systemgrenzen der Schutzebenen liegt (z. B. der Ausfall der Stromversorgung). Diese Definition von Unabhängigkeit ist deutlich strenger als die Kriterien für Sicherheitsschichten. In vielen Fällen führen die strengen USE-Kriterien dazu, dass mehrere (wenn nicht sogar alle) Schutzebenen eines Systems zu einer einzigen USE zusammengefasst werden. Gerade im Bereich der Eisenbahn, wo vollständige Unabhängigkeit im Allgemeinen nicht vorkommt (siehe 3.3.1), würde die Arbeit mit dem Begriff USE dazu führen, dass die Systeme nur sehr grob betrachtet werden. Die meisten (Teil-)Systeme im Bereich der Eisenbahn hätten nur eine einzige unabhängige Schutzebene (USE).

[2] Die Analyse von USE erfolgt stets Szenario-bezogen.

Ein dritter, der Sicherheitsschicht vermeintlich sehr ähnlicher Begriff ist **Defence-in-Depth** (Abschnitt 2.3.2). Beim Konzept der Defence-in-Depth werden Maßnahmen zur Vermeidung von Unfällen und ihren Folgen hierarchisch in fünf Leveln eingesetzt. Erst wenn ein Level versagt, kommen die nachfolgenden Level ins Spiel. Hier besteht ein großer Unterschied zum Konzept der Sicherheitsschichten. Alle Sicherheitsschichten wirken gleichzeitig und gemeinsam, nicht nacheinander. Bei Defence-in-Depth soll ein unerwünschter Ereignisverlauf möglichst bereits durch den ersten Level aufgehalten werden. Bei Sicherheitsschichten besteht diese Anforderung nicht. Es ist nicht von Bedeutung, die wievielte Sicherheitsschicht die Gefährdung verhindert. Demzufolge haben Sicherheitsschichten auch keine festgelegte Reihenfolge.

3.4 Eigenschaften von Sicherheitsschichten

Nachdem in Abschnitt 3.3 die Unterschiede zwischen Sicherheitsschichten und anderen Begriffen dargestellt wurden, werden im Folgenden die Eigenschaften von Sicherheitsschichten, die sich aus ihrer Definition ergeben, noch einmal zusammengefasst.

Sicherheitsschichten *beinhalten Barrieren*. Der Begriff der Barriere (Abschnitt 3.2.2) ist ein sehr weit gefasster Begriff, der ganz verschiedene Mittel beinhalten kann. Dies ist wichtig, denn Sicherheitsmaßnahmen im Bereich der Eisenbahn können ganz verschiedener Natur sein und sollen durch das Konzept der Sicherheitsschichten nicht eingeschränkt werden. Daher kommen als Barrieren von Sicherheitsschichten nicht nur die klassischen materiellen bzw. physischen Barrieren, wie z. B. Absperrungen oder Wände, in Frage. Barrieren können auch symbolisch sein (z. B. Schilder) oder organisatorisch (z. B. Regelwerke). Auch der Mensch kann die Rolle einer Barriere übernehmen.

Sicherheitsschichten sind stets bezogen auf eine *bestimmte Gefährdung*. Ohne den Kontext der Gefährdung, deren Risiko mittels einer Sicherheitsschicht reduziert werden soll, ist eine Sicherheitsschicht unvollständig. Es gibt Sicherheitsschichten, die gegen mehrere Gefährdungen wirken, aber auch solche, die nur gegen eine einzige Gefährdung wirken. Entsprechend gibt es Sicherheitsschichten, die in bestimmten Situationen besonders gut oder eher schlecht wirken. Es ist die Aufgabe der Systementwickler, verschiedene Möglichkeiten zu vergleichen und für ihr System die geeignetsten Sicherheitsschichten auszuwählen.

Sicherheitsschichten sind ein *Teil eines Gesamtsystems*, beschreiben dieses Gesamtsystem aber nicht vollständig. Sicherheitsschichten können einzeln bzgl. ihrer Qualität, ihrer Leistungsfähigkeit und damit bzgl. ihres Sicherheitsgewinns bewertet werden. Die Bewertung kann aber auch für das Gesamtsystem als Ganzes erfolgen.

Sicherheitsschichten sind *voneinander unabhängig*. Dadurch haben sie die Eigenschaft, dass sie einzeln und unabhängig voneinander hinzugefügt oder entfernt werden können, ohne die anderen Sicherheitsschichten des Systems bzgl. ihrer Funktion oder technischen Implementierung zu beeinflussen. Insbesondere beeinflusst das Entfernen einer Sicherheitsschicht nicht die Wirksamkeit der noch verbleibenden Sicherheitsschichten.

Sicherheitsschichten haben stets Schwächen, sie sind *nicht perfekt*. Eine Sicherheitsschicht bietet keinen 100%igen Schutz vor einer Gefährdung. Dies gilt für Sicherheitsschichten genauso wie für alle anderen Arten von Sicherheitsmaßnahmen. Allerdings kann eine Eigenschaft, die auf den ersten Blick als Schwäche erscheint, auch eine Stärke sein. Ein Beispiel hierfür sind Halbschranken an einem Bahnübergang. Eine ihrer Schwächen ist es, dass Verkehrsteilnehmer den Bahnübergang ohne größere Anstrengung auch dann betreten können, wenn die Halbschranken geschlossen sind. Halbschranken ermöglichen es aber auch, dass Verkehrsteilnehmer den Bahnübergang selbst bei geschlossenen Halbschranken noch verlassen können. Dies ist eine der Stärken der Halbschranken.

3.5 Verwendbarkeit von Sicherheitsschichten

3.5.1 Modellierung von Sicherheitsmaßnahmen

Sicherheitsschichten sind geeignet, um die Maßnahmen, die die Sicherheit eines Systems erhöhen, zu benennen, zu modellieren und zu beschreiben. Maßnahmen, die die Sicherheit eines Systems erhöhen, sind Maßnahmen, die das Risiko reduzieren. Das bedeutet, mit Sicherheitsschichten können Maßnahmen, die das Risiko für das Eintreten bestimmter unerwünschter Ereignisse reduzieren, modelliert werden. Allerdings sind nicht alle diese Maßnahmen Sicherheitsschichten. Mit Sicherheitsschichten werden also nur bestimmte Maßnahmen modelliert. Dies sind diejenigen, die sich aufgrund ihrer Unabhängigkeit in ihrer Wirkung addieren. Es sind die *wesentlichen Maßnahmen*.
Die Modellierung durch Sicherheitsschichten geschieht am besten auf einer relativ hohen Systemebene, d. h. nicht auf der Ebene von Bauteilen, Schaltkreisen und Relais, aber auch nicht auf einer Gesamtsystemebene wie „ein Zug“ oder „ein Stellwerk“. Die Anwendung des Konzepts der Sicherheitsschichten erfolgt zwischen diesen beiden Extremen. Der Nutzer des Modells kann dabei in einem gewissen Rahmen die Ebene seinen Bedürfnissen anpassen – je nachdem was er untersuchen oder darstellen möchte. Begrenzt ist der Anwendungsbereich eines Modells der Sicherheitsschichten nur durch die Sinnhaftigkeit und durch die Unabhängigkeitskriterien aus Abschnitt 3.2.5. Sinnhaftigkeit meint: Ein System, das so grob modelliert wird, dass es nur eine Sicherheitsschicht hat, kann zwar seine Sicherheitsmaßnahmen durch diese eine Sicherheitsschicht beschreiben. Einen wirklichen Nutzen hat das Modell jedoch erst dann, wenn es aus mehreren Sicherheitsschichten besteht. Die Unabhängigkeitskriterien beschränken die Anwendung des Modells vor allem bzgl. der Detaillierungsebene. Auf der Ebene von Schaltkreisen oder Recheneinheiten ist die Unabhängigkeit oft nicht mehr gegeben, hier macht es keinen Sinn, die Sicherheitsmaßnahmen noch in Sicherheitsschichten weiter untergliedern zu wollen.
Gut geeignet ist eine funktionale Ebene wie beim Ansatz der CENELEC-Normen, möglichst noch ohne detaillierte Umsetzungsvorgaben, also wenn noch nicht feststeht, ob ein Relais mit vier oder acht Kontakten verwendet wird, von welcher Firma das Bauteil ist etc.

3.5.2 Vergleich von Sicherheitsmaßnahmen

Sicherheitsschichten können verwendet werden, um die Sicherheitsmaßnahmen neuer Entwürfe zu modellieren und mit denen anderer Entwürfe zu *vergleichen*. Dieser Vergleich ist aufgrund der Unabhängigkeitskriterien leicht möglich. Durch die Unabhängigkeitskriterien werden die Sicherheitsmaßnahmen so modelliert, dass die Unterschiede verschiedener Entwürfe an klar abgegrenzten Sicherheitsschichten sichtbar werden, z. B. durch das Vorhandensein von mehr oder weniger Sicherheitsschichten oder durch die unterschiedliche Güte von Sicherheitsschichten (mehr oder weniger Schwächen). Dies ermöglicht auch die Darstellung und den Vergleich der unterschiedlichen Sicherheitsniveaus in verschiedenen Systemen – ein nützliches, wenngleich auch nicht immer erwünschtes Wissen auf dem Weg zu einer europäischen Harmonisierung.

3.5.3 Bewertung von Änderungen an Systemen

Heutzutage werden in Europa nur noch selten Strecken / Bahnsysteme komplett neu gebaut. Weitaus häufiger werden Änderungen an bestehenden Systemen vorgenommen. Hierbei ist es wichtig, bereits im Vorfeld beurteilen zu können, wie sich die geplanten Änderungen auf die Sicherheit auswirken. Das Konzept der Sicherheitsschichten bietet hier eine gute Grundlage für diese Analyse. Sicherheitsschichten eines im Entwurf befindlichen Systems können verändert oder ausgetauscht und das Ergebnis bewertet werden.

Wenn über die Änderungen entschieden wurde, müssen die Änderungen in der Regel[3] von einer zulassenden Behörde genehmigt werden. Hierzu wird üblicherweise aus Gründen der Kostenersparnis eine sogenannte *Delta-Betrachtung* vorgenommen. Bei einer Delta-Betrachtung wird nicht das gesamte System neu bewertet, sondern lediglich die Änderungen. Dabei ist es wichtig, sowohl die Änderungen selbst, als auch die Rückwirkungsfreiheit auf das übrige System und ggf. auch benachbarte Systeme hinsichtlich der Auswirkungen auf die Sicherheit zu bewerten. Das Budget für solche Änderungsbegutachtungen ist in der Regel relativ gering, sodass der Gutachter / die zulassende Behörde vor der Herausforderung stehen, innerhalb kurzer Zeit die Auswirkungen einer Änderung auf ein mitunter sehr komplexes System zu erfassen und zu bewerten. Besonders aufwändig und schwierig ist dabei die Frage der Rückwirkungsfreiheit zu beantworten.
Erschwerend kommt hinzu, dass die Dokumentation des ursprünglichen Systems und seiner Änderungen meist in einer Form vorliegt, die für eine solche Bewertung schlecht geeignet ist: in Form von Fließtext, mit geringer Strukturierung hinsichtlich der Sicherheitsaspekte und nur rudimentären Schnittstellenbeschreibungen. Formale Auswirkungsanalysen liegen selten vor. Der Grund hierfür liegt darin, dass die Systemdokumentation vom Hersteller erstellt wurde, um ein System zu beschreiben, das bestimmte (vor allem betriebliche) Funktionen erfüllt. Die Dokumentation wird (aus verständlichen Gründen) nicht so aufgebaut, dass sich zukünftige Änderungen gut einpflegen lassen. Vor allem aber dient die Dokumentation dem Bau des Systems und weniger der Sicherheitsbewertung. Die Dokumentation zur Sicherheitsbewertung (z. B. Berechnung von Ausfallraten, Fehler-Möglichkeits- und Einfluss-Analyse (FMEA), Sicherheitsnachweise etc.) wird aus Sicht des Herstellers meist als notwendiges Übel ohne echten Mehrwert angesehen und entsprechend behandelt.
Eine Modellierung der Sicherheitsmaßnahmen des Systems in Form von Sicherheitsschichten würde die Änderungsbegutachtungen deutlich erleichtern. Die Änderungen können einer oder mehreren Sicherheitsschichten zugeordnet werden. Durch die Unabhängigkeitskriterien können die Auswirkungen der Änderungen leichter abgeschätzt werden. Die Frage nach der Rückwirkungsfreiheit kann in einem gewissen Rahmen leicht beantwortet werden (Ausnahme: CCF). Dadurch muss der Prüfer nur noch Teile des Systems betrachten und hat eine klare Struktur als Arbeitsgrundlage.

3.5.4 Weitere Verwendungsmöglichkeiten

Ein Modell der Sicherheitsschichten eines Systems ist auch eine gute *Grundlage für eine quantitative Betrachtung der Sicherheit*. Die Sicherheitsschichten werden durch Sicherheitsbarrieren und ihre Funktionen beschrieben. Das sind genau die Elemente, die bei einer quantitativen Analyse von Interesse sind. Sind alle Sicherheitsschichten eines Systems bekannt, kann bei einer quantitativen Analyse Aufwand gespart werden. Da das Modell auf einzelne Gefährdungen bezogen ist, wird die Berechnung von Gefährdungsraten erleichtert. Durch die Unabhängigkeitskriterien werden wertvolle Informationen zur Erstellung von Fehlerbäumen und anderen Modellen zur quantitativen Analyse gegeben.
Bevor neue oder geänderte Bahnsysteme in Betrieb gehen dürfen, muss in der Regel ein *Sicherheitsnachweis* vorliegen. In jedem Sicherheitsnachweis gemäß DIN EN 50129 [DIN03] muss ein Abschnitt zum Thema „Unabhängigkeit von Betrachtungseinheiten“ enthalten sein. Die Sicherheitsschichten bilden hierfür aufgrund ihrer Unabhängigkeitskriterien eine wertvolle Grundlage.
Ein weiterer Vorteil der Modellierung von Sicherheitsmaßnahmen durch Sicherheitsschichten ist die leichte Verständlichkeit des Konzepts. Insbesondere zusammen mit einer bildlichen Darstellung erleichtert das Modell die *interdisziplinäre Kommunikation*. Dies ist wichtig, wenn die Sicherheitsmaßnahmen auch Nicht-Experten vorgestellt werden sollen, z. B. Politikern, Fachleuten aus angrenzenden Fachbereichen, Richtern oder der Öffentlichkeit.

[3] Ausnahme: Die Änderungen sind marginal und beeinflussen keine sicherheitsrelevanten Elemente des Systems.

4 Modelle und Darstellungsweisen

Ein Sprichwort sagt: *Ein Bild sagt mehr als tausend Worte*. Für die in Abschnitt 2.3 aufgeführten Begriffe, insbesondere für Barrieren und Schutzebenen, gibt es verschiedene Modelle und Darstellungsweisen (Beschreibungsmittel), die der Veranschaulichung dieser Begriffe dienen.
Im Folgenden wird eine Auswahl der vorhandenen Darstellungsweisen für Barrieren, Schutzebenen und ähnliche Begriffe präsentiert. Die Auswahl erfolgte auf Basis einer Literaturrecherche, passend zu den in Abschnitt 2.3 vorgestellten Begriffen und mit Hinblick auf das Ziel der Darstellung von Sicherheitsschichten (Kapitel 3). Zu jeder Darstellungsweise werden die wichtigsten Vor- und Nachteile diskutiert, um am Ende entscheiden zu können, welche Darstellungsform für Sicherheitsschichten in Eisenbahnsystemen, unter Berücksichtigung von Ziel und Zweck der vorliegenden Arbeit, am besten geeignet ist.
Die Darstellungsweise ist bedeutsam, denn eine gute bildliche Darstellung trägt viel zum Erfolg eines Konzepts bei. Gerade weil Sicherheit ein sehr abstrakter Begriff ist, ist eine bildliche Darstellung hilfreich, um über dieses schwer greifbare Thema sprechen zu können. Sicherheit kann man weder anfassen noch sehen oder messen. Messbar hingegen sind Unfälle, Vorfälle oder Ausfälle von Systemkomponenten. Diese Ereignisse entsprechen jedoch dem Gegenteil von Sicherheit. Man misst Sicherheit für gewöhnlich, indem man ihr Gegenteil misst bzw. abschätzt: durch das Risiko [LSKM, SS10], denn Sicherheit bezeichnet das „Nichtvorhandensein eines unzulässigen Schadensrisikos“[DIN00].
Gerade im Bereich der Sicherheit ist es wichtig, dass Fachleute verschiedener Disziplinen (Ingenieure verschiedener Fachrichtungen, Entwickler, Bediener, Betreiber, Gutachter, Behörden, Politiker, Juristen, Manager, Finanzfachkräfte etc.) miteinander sprechen und einander verstehen. Bildliche Darstellungen haben daran einen wesentlichen Anteil. Allerdings darf nicht vergessen werden, dass jedes Bild beim Betrachter bestimmte Assoziationen weckt, wie seine Elemente zusammenhängen. Je nach gewählter Darstellungsweise wird der Betrachter auf Probleme gelenkt oder auch von ihnen abgelenkt. Ein Bild baut auf dem mentalen Modell auf, das der Zeichner von seinem System und von den Zusammenhängen hat. So basieren alle Darstellungen von Sicherheitsschichten, Barrieren und ähnlichen Begriffen auf einer Vorstellung / einem Modell, wie es zu gefährlichen Vorfällen / Unfällen kommt und wie man sie verhindern kann.
Es gibt zahlreiche Darstellungsweisen und ständig wächst ihre Zahl, da jede Domäne ihre ganz speziellen Anforderungen und Schwerpunkte hat und ihre eigenen Zwecke verfolgt. So gibt es immer wieder maßgeschneiderte Lösungen für einzelne Bereiche. Daher werden zunächst die Anforderungen an eine geeignete Darstellungsweise für Sicherheitsschichten definiert.

4.1 Anforderungen an die Darstellungsweise

Mit Hinblick auf das Ziel dieser Arbeit und insbesondere die in Kap. 3 beschriebenen Anforderungen und Eigenschaften von Sicherheitsschichten, sollte eine gute Darstellungsweise den folgenden Anforderungen genügen. Sie soll

- D-1 eine begrenzte Komplexität aufweisen, d. h. einfach sein und nur wenige Symbole verwenden, um die Anwendung zu erleichtern
- D-2 verständlich, möglichst eindeutig und intuitiv richtig zu interpretieren sein, um die interdisziplinäre Kommunikation zu unterstützen (Abschnitt 3.5.4)

D-3 auf mehreren Detaillierungstiefen flexibel anwendbar sein, um den Analysten bei einer flexiblen und seinen Bedürfnissen entsprechenden Modellierung zu unterstützen (Abschnitt 3.5.1)

D-4 alle Arten von Systemelementen darstellen können: technische, menschliche, organisatorische etc., da auch Sicherheitsschichten diese Aspekte umfassen (Anforderungen S-7 und S-8, Abschnitt 3.1)

D-5 explizit Barrieren oder ähnliche Elemente (Abschnitt 2.3) enthalten, da Sicherheitsschichten Barrieren enthalten (Abschnitt 3.2)

D-6 den zeitlichen Verlauf der Ereignisse berücksichtigen, um die Nachvollziehbarkeit zu erhöhen

D-7 den kausalen Zusammenhang der Ereignisse berücksichtigen, da der Zusammenhang zwischen Ursachen und Folgen für das Verständnis der Sicherheit eines Systems von großer Bedeutung ist

D-8 die Ursache(n) für den Eintritt eines Ereignisses beinhalten, um die explizite Darstellung des kausalen Zusammenhangs zu ermöglichen

D-9 die Folge(n) eines Ereignisses beinhalten, um die explizite Darstellung des kausalen Zusammenhangs zu ermöglichen und um den Bezug der Sicherheitsschichten auf Gefährdungen sichtbar zu machen (Anforderung S-12, Abschnitt 3.1)

D-10 zur Darstellung von Unfällen einsetzbar sein, um den Rückfluss von Erkenntnissen aus Unfallanalysen in das Modell der Sicherheitsschichten zu unterstützen

D-11 präventiv, d. h. bereits vor einem Unfall einsetzbar sein, um die Verwendbarkeit des Konzepts der Sicherheitsschichten für Sicherheitsnachweise zu unterstützen (Anforderung S-3, Abschnitt 3.1)

4.2 Energiemodell

Ein weit verbreitetes und viel genutztes Modell zur Beschreibung von Unfällen und Gegenmaßnahmen ist das *Energiemodell*. Dieses Modell stammt ursprünglich aus dem Bereich der Medizin und geht auf Gibson und Haddon zurück [HR01]. Das Energiemodell geht davon aus, dass die Quelle eines Schadens für den Menschen (oder die Umwelt oder ein technisches System[1]) eine Form von Energie ist. Diese Energie kann z. B. thermisch, kinetisch, nuklear oder elektrisch sein. Der Mensch kann durch diese Energie Schaden nehmen. Um dies zu verhindern, muss der Mensch durch Barrieren vor der Energie geschützt werden (Abbildung 4.1).

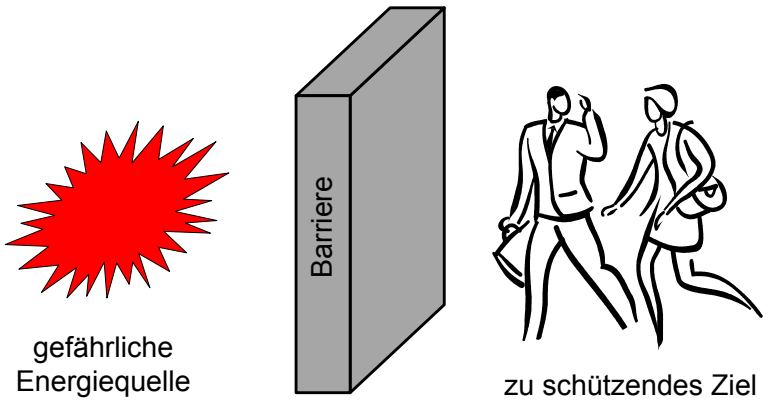

Abbildung 4.1: Energiemodell in Anlehnung an Sklet [Skl06]

[1] Im Folgenden wird nur der Schaden für den Menschen betrachtet. Die Modelle und Konzepte lassen sich aber genauso auf Umweltschäden, Sachschäden und andere Schäden anwenden.

Haddon veröffentlichte 1973 zehn Strategien gegen Schaden, der von Energie ausgeht [Had95]. Diese Strategien reichen vom Verhindern, dass die Energie entsteht, über die zeitliche / räumliche Trennung von Energie und Mensch, dem Platzieren materieller Barrieren zwischen der Energie und dem Menschen, bis hin zur Schadenserkennung und -behebung. Haddons zehn Strategien wurden seitdem angepasst und erweitert. So verwendet Ericson [Eri05] bereits zwölf. Diese Strategien sind heute die Grundlage für viele sicherheitsbezogene Betrachtungen, z. B. im Bereich der Verkehrssicherheit. Insbesondere das Konzept der Barrieren (Abschnitt 2.3.1) wird gern verwendet, um Sicherheitsmaßnahmen darzustellen, und das Konzept der Barrieren verwendet in der Regel implizit das Energiemodell.

Vor- und Nachteile des Energiemodells:

Das Energiemodell ist ein Basis-Modell. Es veranschaulicht auf einfache und intuitive Weise ein Prinzip: Das Schützen des Menschen vor schädlicher Energie durch Barrieren. Es ist die Basis für zahlreiche andere Modelle und Darstellungsweisen, z. B. für das Schweizer-Käse-Modell von Reason [Rea04]. Dadurch, dass das Energiemodell eine Prinzipdarstellung ist, lassen sich einzelne, einfache Situationen und Barrieren darstellen. Um komplexe Systeme und ihre Schutzmechanismen detailliert zu beschreiben, ist es jedoch nicht geeignet. Das Energiemodell als Prinzipdarstellung ist nicht nur in der Medizin, sondern auch im Bahnbereich anwendbar. Im Bahnbereich entstehen Schäden vor allem durch kinetische Energie – sich bewegende Züge – und thermische Energie, z. B. brennbare Güter. Ein energiebezogener Ansatz bietet die Möglichkeit, Sicherheitsmaßnahmen entsprechend dem vorhandenen energetischen Schadenspotenzial zu verwenden. Weber [Web10] hat diese Idee bereits für den Zugleitbetrieb aufgegriffen. Um diesen Ansatz im Bahnbereich jedoch durchgehend anwenden zu können, bedarf es noch weiterer Grundlagenarbeit, z. B. mit Hinblick auf die entsprechende Mathematik und Physik.

4.3 Zwiebelschalenmodell

Das *Zwiebelschalenmodell (ZSM)* wird zur Darstellung von *Defence-in-Depth* (Abschnitt 2.3.2) und *Schutzebenen* (Abschnitt 2.3.3) verwendet und wird auch in der DIN EN 61511-1 [DIN05a] beschrieben. Im Zentrum der Darstellung steht ein Prozess, der, wenn er außer Kontrolle gerät, eine Gefährdung darstellt. Ringförmig um den Prozess herum, so wie die Schalen einer Zwiebel, sind verschiedene Schutzebenen dargestellt (Abbildung 4.2). Dabei sind die inneren Schutzebenen auch in der Realität näher am Prozess und können auf ihn einwirken und ihn kontrollieren. Je weiter außen die Schutzebenen liegen, desto weniger Einfluss können sie auf den Prozess nehmen. Ihre Funktion entfernt sich mehr und mehr von der Kontrolle des Prozesses, hin in Richtung Reduzierung des Schadens durch Maßnahmen, die den Menschen direkt schützen. Die ganz außen liegenden Schutzebenen schließlich gehören nicht dem Prozesseigner selbst, sondern der Allgemeinheit.
Wenn es zu einem unerwünschten Ereignis im Prozess kommt, soll zunächst die innerste Schutzebene greifen. Erst wenn die erste Schutzebene versagt, kommt die zweite zum Tragen usw. Je weiter außen die Schutzschichten liegen, desto größer ist das bereits entstandene Problem.
Die DIN EN 61511-1 [DIN05a] nennt fünf typische Schutzebenen und stellt sie in Form eines Zwiebelschalenmodells dar:

1. „Regelung und Überwachung“[2] (des Prozesses)
2. „Schutz“ (mit sicherheitstechnischen Systemen)
3. „Schadensbegrenzung“ (z. B. mit mechanischen Systemen, durch Alarme, Bedienereingriffe)
4. „Anlagenbezogene Maßnahmen in Notfällen“ (z. B. Evakuierungsmaßnahmen)
5. „Öffentliche Maßnahmen in Notfällen“ (z. B. mit Hilfe von Rundfunk)

[2] Zitate aus [DIN05a]

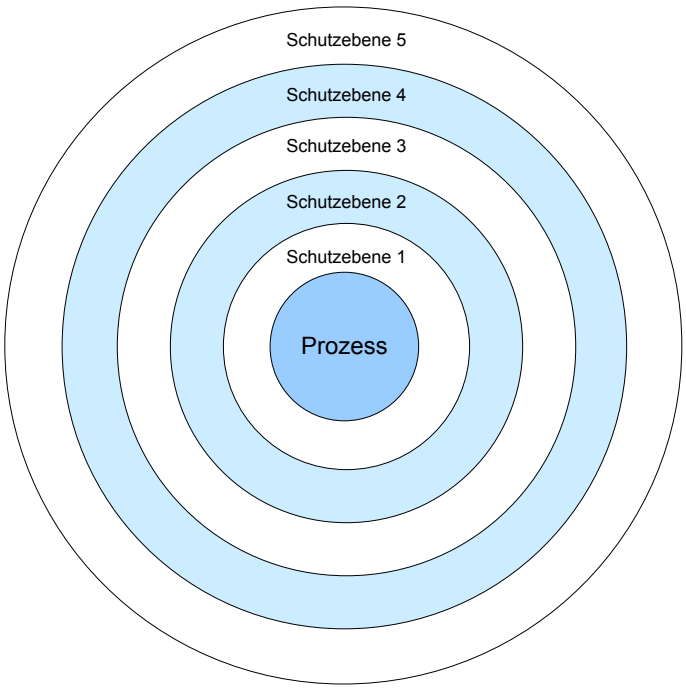

Abbildung 4.2: Zwiebelschalenmodell nach Börcsök [BÖ6]

Vor- und Nachteile des Zwiebelschalenmodells:

Das Zwiebelschalenmodell veranschaulicht gut die Eskalation, die ein außer Kontrolle geratener Prozess mit sich zieht. Es stellt durch die Größe und die Anordnung der Zwiebelschalen gut dar, wie die räumliche Ausdehnung des Problems nach und nach wächst, wie mehr und weiter entfernte Personen und Anlagen betroffen werden, und wie der Aufwand für den Schutz dieser Personen und Anlagen steigt, wenn die inneren Schutzebenen versagen. Auch das Basisprinzip, das Eindämmen frei werdender Energie, wird durch die kreisförmige Darstellung unterstrichen. Die Darstellung ist einfach und intuitiv richtig zu verstehen, enthält aber weder konkrete Folgen noch Gefährdungen. Durch die geschlossen gezeichneten Kreise wird jedoch auch leicht der Eindruck erweckt, die Schutzebenen wären in der Lage, einen perfekten Rundumschutz zu gewährleisten. Das Zwiebelschalenmodell lässt sich prinzipiell auf verschiedenen Detaillierungsebenen anwenden, ist durch die typischen Schutzebenen aus der DIN EN 61511-1 [DIN05a] jedoch in der Praxis bzgl. der Detaillierungsebene vorgeprägt.

4.4 Layer-of-Protection-Analysis-Diagramm (LOPA-Diagramm)

Das *Layer-of-Protection-Analysis-Diagramm (LOPA-Diagramm)* [BÖ6] stellt das Schutzebenenkonzept eines Systems in Anlehnung an einen Ereignisbaum (siehe [DIN11d]) dar. Im Unterschied zu einem Ereignisbaum wird nur der Pfad für den negativen Fall, d. h. das Versagen der unabhängigen Schutzebene (USE) (Abschnitt 2.3.3), dargestellt.
Im LOPA-Diagramm werden die unabhängigen Schutzebenen durch Blöcke dargestellt. Störungen / Ausfälle werden durch Pfeile symbolisiert. Die zeitliche und kausale Ereignisabfolge entwickelt sich entlang der Pfeilrichtung von links nach rechts. Jede USE hat die Möglichkeit, den Ereignisverlauf zu stoppen. Durch die Dicke der Pfeile wird dargestellt, wie sich die Wahrscheinlichkeit für das Eintreten des unerwünschten Ereignisses durch die vor dem Pfeil liegende USE verringert: Die Dicke der Pfeile nimmt von links nach rechts ab bis noch eine Restwahrscheinlichkeit übrig bleibt. Durch die Länge der Pfeile kann zusätzlich das Ausmaß des zu erwartenden Schadens dargestellt werden.

Im LOPA-Diagramm in Abbildung 4.3 wird durch die USE nur die Wahrscheinlichkeit, nicht aber das Schadensausmaß verringert: Alle Pfeile sind gleich lang.

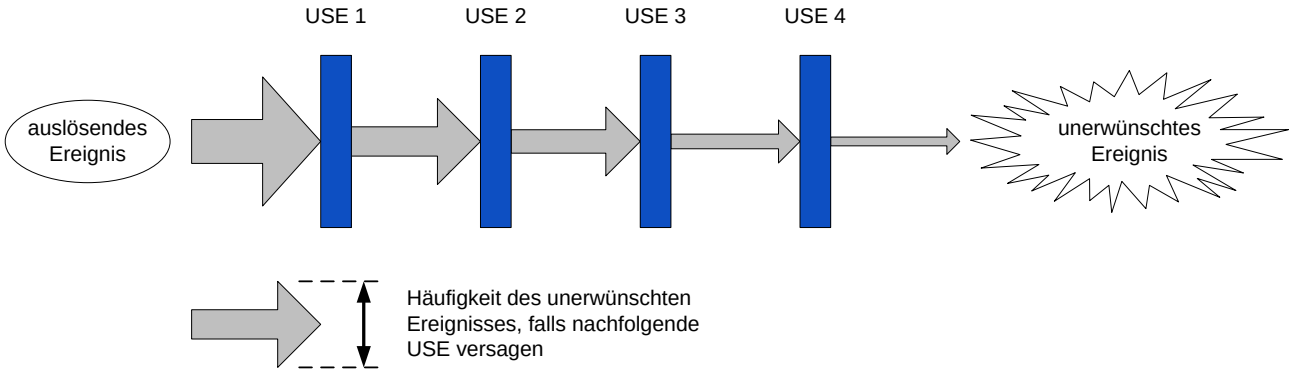

Abbildung 4.3: Layer-of-Protection-Analysis-Diagramm (LOPA-Diagramm) in Anlehnung an Börcsök [B06] und CCPS [Cen01] (Beispiel)

Vor- und Nachteile des LOPA-Diagramms:

Im Vergleich zum Zwiebelschalenmodell kann im LOPA-Diagramm zusätzlich zu den Schutzebenen auch deren risikoreduzierende Wirkung durch die Breite und Länge der Pfeile dargestellt werden. Dadurch werden die Darstellungsmöglichkeiten erweitert, aber die Bedeutung von Pfeillänge und -dicke ist intuitiv nicht mehr ohne weiteres zu verstehen bzw. wird bisweilen nicht erkannt. Dadurch dass auch rechts von der letzten USE ein ausgehender Pfeil dargestellt ist, wird der Eindruck vermieden, dass die USE einen perfekten Rundumschutz ermöglichen. Durch die Darstellung als einzeln stehende Blöcke wird die Unabhängigkeit der USE verdeutlicht.
Das LOPA-Diagramm ist auf seinen Anwendungsbereich, die Prozessindustrie, zugeschnitten: Es werden nur *unabhängige* Schutzebenen (USE) in das Diagramm aufgenommen. Die USE wirken in der Reihenfolge, in der sie gezeichnet sind, von links nach rechts. Ein LOPA-Diagramm kann für jede Detaillierungsebene, auf der sich USE befinden, gezeichnet werden.

4.5 Dominomodell

Das *Dominomodell*, auch als Dominotheorie bekannt, geht auf Heinrich zurück, der zehn Axiome industrieller Sicherheit aufstellte [HPR80]. Besonders prägend für das gängige Unfallursachenmodell in der Mitte des 20. Jahrhunderts war das erste dieser Axiome. Es besagt, dass ein Schadenereignis das Resultat einer Sequenz von Faktoren ist, von denen der letzte der Unfall selbst ist. Dieser Gedankengang wird durch das Dominomodell dargestellt. Es besteht laut Heinrich [HPR80] aus den folgenden fünf Dominosteinen (siehe auch Abbildung 4.4):

1. „Ancestry and social environment“ – Abstammung und soziales Umfeld[3] (Persönlichkeit der Arbeiter)
2. „Fault of person“ – menschlicher Fehler (Charakterzug)
3. „Unsafe act and/or mechanical or physical hazard“ – unsichere Handlung und / oder mechanische oder physische Gefährdung
4. „Accident“ – Unfall
5. „Injury“ – Schaden (Verletzung von Menschen)

[3]Zitate aus [HPR80], übersetzt durch die Autorin

Die Dominosteine symbolisieren die fünf Faktoren, ihr Fallen die Unfallsequenz. Dabei stehen die Steine zueinander in einer Ursache-Wirkungs-Beziehung. Fällt der erste Stein, so stößt er die anderen an, sodass sie ebenfalls fallen. Wenn ein Dominostein fehlt, wird die Unfallsequenz unterbrochen, die verbleibenden Steine fallen nicht – es kommt nicht zum Unfall.

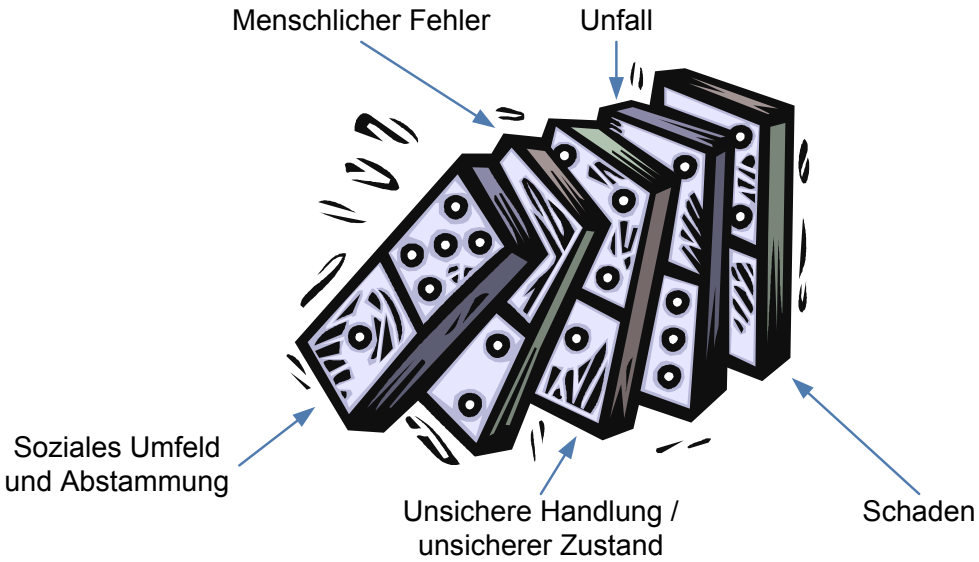

Abbildung 4.4: Dominomodell nach Heinrich [HPR80]

Vor- und Nachteile des Dominomodells:

Das Dominomodell veranschaulicht wie das Energiemodell auf einfache Weise ein Prinzip: dass die unmittelbare Ursache eines Unfalls selbst auch wieder Ursachen hat. Es legt dabei großen Wert auf die Betrachtung des Menschen als Teil des Systems und beachtet dabei auch das soziale Umfeld und die (Unternehmens-)Kultur. Das Dominomodell veranschaulicht die ganze Sequenz, die einem Unfall vorausgeht. Durch die Fokussierung auf die Sequenz von negativen Faktoren, die zu einem Unfall führen, unterscheidet es sich grundlegend von anderen Modellen, die sich auf die Darstellung von positiven Sicherheitsmaßnahmen konzentrieren. Die sequenzhafte Darstellung verleitet zu der Annahme, dass jeder Unfall eine einzige Grundursache besitzt und lenkt die Bemühungen zur Verbesserung der Sicherheit dahin, genau diese Grundursache zu beseitigen. Unfallursachenanalysen, die nach dem heutigen Stand von Wissenschaft und Technik durchgeführt werden, gehen jedoch davon aus, dass ein Unfall in der Regel mehr als das Resultat eines einzigen „Problems“ ist. Vielmehr müssen – insbesondere bei komplexen sicherheitsrelevanten Systemen – in der Regel mehrere Ursachen zusammenkommen, damit ein Unfall geschehen kann. Ein weiterer Nachteil des Dominomodells ist die starke Fokussierung auf den Menschen und seine Fehler als Schwachstelle des Systems. Das Modell vernachlässigt dabei die technischen und organisatorischen Faktoren, die ebenso ihren Beitrag zu Unfällen beisteuern. Im Gegensatz zu anderen, weit verbreiteten Modellen wie dem Zwiebelschalenmodell (Abschnitt 4.3) oder dem LOPA-Diagramm (Abschnitt 4.4) stellen die Dominosteine keine positiven Maßnahmen gegen einen Unfall dar, sondern negative Aspekte, die zu einem Unfall führen. Daher werden Fachleute, die diese anderen Modelle kennen, das Dominomodell zunächst falsch interpretieren. Die Darstellung ist daher nicht ganz intuitiv, sondern bedarf einer Erläuterung.

4.6 Schweizer-Käse-Modell (Swiss Cheese Model)

Das *Schweizer-Käse-Modell (SCM)* von Reason [Rea04] greift die ursprüngliche Darstellung des Energiemodells (Abschnitt 4.2) auf, in der Barrieren vor einer Gefährdung schützen. Im Gegensatz zu anderen Modellen werden die Barrieren nicht perfekt, sondern mit Löchern dargestellt – wie hintereinander liegende Käsescheiben (Abbildung 4.5). Die Löcher stellen die Unvollkommenheit der Barrieren dar, denn keine Barriere bietet 100 %igen Schutz.

Im Gegensatz zum Dominomodell (Abschnitt 4.5) und dem LOPA-Diagramm (Abschnitt 4.4) wird hier jedoch keine zeitliche Sequenz ausgedrückt. Die Barrieren dienen dem Schutz vor unerwünschten Ereignissen – insbesondere vor Unfällen. Da die meisten Unfälle heutzutage nicht das Resultat eines einzigen fatalen Fehlers sind, sondern mehrere Ursachen haben, verwendet das Modell zur Darstellung der Sicherheitsmaßnahmen nicht eine schützende Barriere, sondern mehrere. Bevor es zu einem Unfall kommen kann, müssen sämtliche hintereinander liegende Barrieren durchbrochen werden. Dabei beschreibt der Pfeil den Unfallhergang: einen Weg durch die Löcher aller hintereinander liegenden Barrieren hindurch.

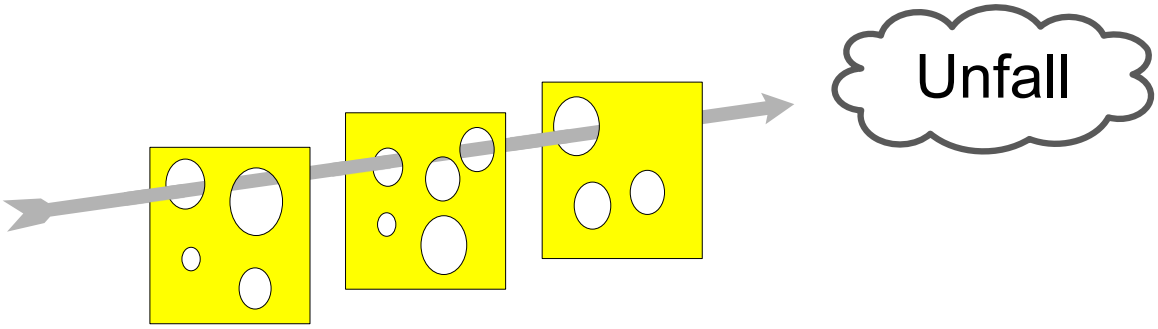

Abbildung 4.5: Schweizer-Käse-Modell nach Reason et al. [RHP06]

Vor- und Nachteile des Schweizer-Käse-Modells:

Das Schweizer-Käse-Modell (SCM) ähnelt, insbesondere in der Darstellung, dem Zwiebelschalenmodell (Abschnitt 4.3) und dem LOPA-Diagramm (Abschnitt 4.4). Der bedeutsamste Unterschied zu diesen beiden Modellen ist, dass der Betrachter darauf gelenkt wird, zu akzeptieren, dass Barrieren unvollkommen sein können. Eine Barriere kann fehlerhaft sein, ausfallen, umgangen werden oder für einen speziellen Fall gar nicht erst ausgelegt worden sein. Die Löcher in den Käsescheiben veranschaulichen, dass bei jeder getroffenen Schutzmaßnahme stets ein Restrisiko verbleibt und es keine absolute Sicherheit geben kann. Dadurch wird die Darstellung etwas komplexer als bei den genannten Modellen, ist aber intuitiv richtig zu interpretieren. Das SCM kann flexibel auf jeder gewünschten Systemebene verwendet werden.

Eine Schwierigkeit bei der Darstellung des SCM auf Papier ist, dass die Löcher der Käsescheiben fix sind. In Wirklichkeit bewegen sie sich jedoch und verändern sogar ihre Größe [Rea04], z. B. wenn eine Käsescheibe durch einen Menschen realisiert wird: Je nachdem, ob es Tag oder Nacht ist, ob der Mensch krank oder gesund ist, und je nachdem, welcher Mitarbeiter gerade die Schicht übernimmt, kann es bei seinen Handlungen zu ganz unterschiedlichen Fehlern / Mängeln kommen. Es können mal mehr und mal weniger, mal schwerwiegendere und mal harmlosere Fehler auftreten. Dementsprechend verändern sich auch die Löcher in den Käsescheiben des Modells. Solche Phänomene treten nicht nur beim Menschen auf, auch technische Systeme sind in ihrer Leistungsfähigkeit Veränderungen unterworfen.

4.7 Fliegendiagramm (Bow-Tie Diagram)

Das *Fliegendiagramm*, besser bekannt unter dem englischen Begriff *Bow-Tie Diagram*, ist von seiner Darstellung her eine Kombination aus einem Fehlerbaum und einem Ereignisbaum [DF06]. Es besteht aus zwei Diagrammteilen, die sich in der Mitte in einem unerwünschten Ereignis (z. B. einem Unfall) treffen (Abbildung 4.6). Auf der linken Seite sind die möglichen Ursachen für das unerwünschte Ereignis in Form eines vereinfachten Fehlerbaums zu finden. Im vereinfachten Fehlerbaum wird auf die sonst üblichen UND- und ODER-Verknüpfungen sowie auf alle anderen Verknüpfungen verzichtet. Die rechte Seite des Fliegendiagramms zeigt die möglichen Folgen des unerwünschten Ereignisses in Form eines vereinfachten Ereignisbaums.

Die Darstellung beschreibt von links nach rechts im Groben einen zeitlichen Ablauf, im Detail ist dieser zeitliche Zusammenhang jedoch nicht immer gegeben.

In ganz einfachen Darstellungen des Fliegendiagramms werden sogar die Verzweigungen, die normalerweise in Fehler- und Ereignisbäumen vorhanden sind, weggelassen. Die möglichen Verläufe werden auf einen Pfeil reduziert. Stattdessen werden Barrieren in das Diagramm eingezeichnet, die den Ereignisverlauf, wie er dem Pfeil folgt, aufhalten oder verändern können (Abbildung 4.6).

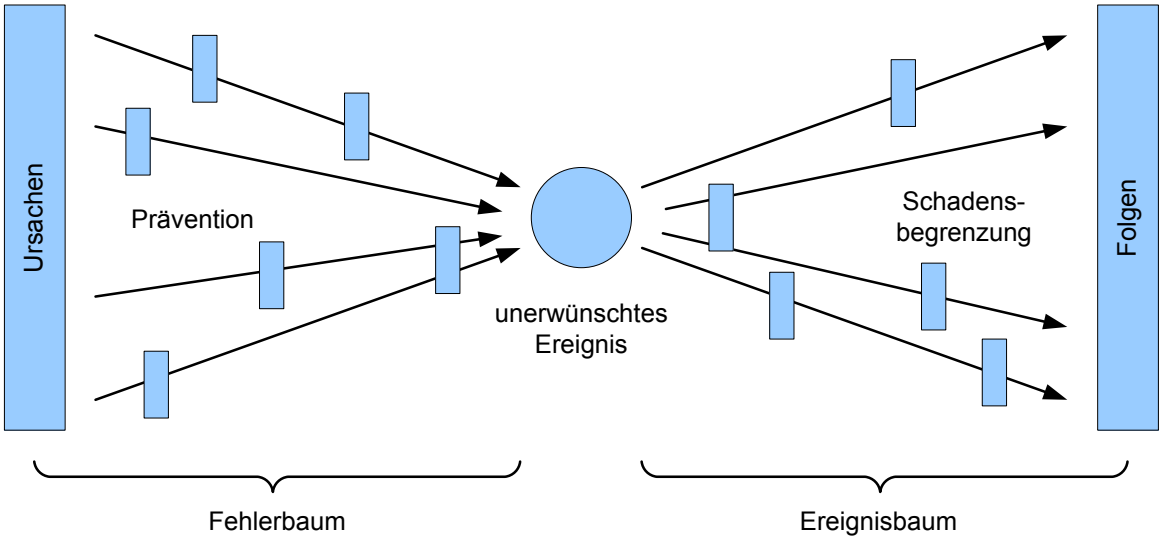

Abbildung 4.6: Fliegendiagramm (Bow-Tie Diagram) in Anlehnung an Dianous et al. [DF06]

Entsprechend dem Unterschied zwischen den beiden Seiten der Fliege, den Ursachen auf der linken und den Folgen auf der rechten Seite, lassen sich auch die eingezeichneten Barrieren in zwei Klassen unterteilen: Die Barrieren auf der linken Seite verhindern das Eintreten des unerwünschten Ereignisses, während die Barrieren auf der rechten Seite den entstehenden Schaden abmildern.

Ebenfalls verbreitet ist eine um 90° gedrehte Variante des Fliegendiagramms, mit dem Ereignisbaum oben und dem Fehlerbaum unten: die „Sanduhr“ (siehe [Mas12]).

Vor- und Nachteile des Fliegendiagramms:

Das Fliegendiagramm ist intuitiv richtig zu verstehen, verschafft sich diesen Vorteil jedoch durch eine vereinfachte Darstellung der Beziehungen zwischen Ursachen und Folgen. Trotz dieser Vereinfachungen ist die Darstellung etwas komplexer, als beispielsweise beim Zwiebelschalendiagramm. Das Fliegendiagramm stellt – im Gegensatz zu vielen anderen Darstellungen – nicht nur mögliche Ursachen für ein Ereignis dar, sondern auch mögliche Folgen. Es ist flexibel auf jeder beliebigen Systemebene einsetzbar.

4.8 Event and Barrier Function Model

Beim *Event and Barrier Function Model (EBFM)* [KEWS96] wird ein Prozess oder eine Aufgabe als eine Abfolge von Ereignissen oder Teilaufgaben modelliert (Abbildung 4.7). Die schwarz umrandeten Kästen beschreiben von links nach rechts den modellierten Prozess. Die rot[4] umrandeten runden Felder darüber beschreiben mögliche Fehler, die dazu führen können, dass das zugehörige Ereignis nicht eintritt oder die zugehörige Teilaufgabe nicht erfüllt wird. Diese Fehler können sowohl technischer Art sein als auch aus dem Bereich der Human Factors stammen. Die blauen Doppelpfeile stellen Barrierefunktionen dar, die negative Auswirkungen des Fehlers auf die Teilaufgabe blockieren.

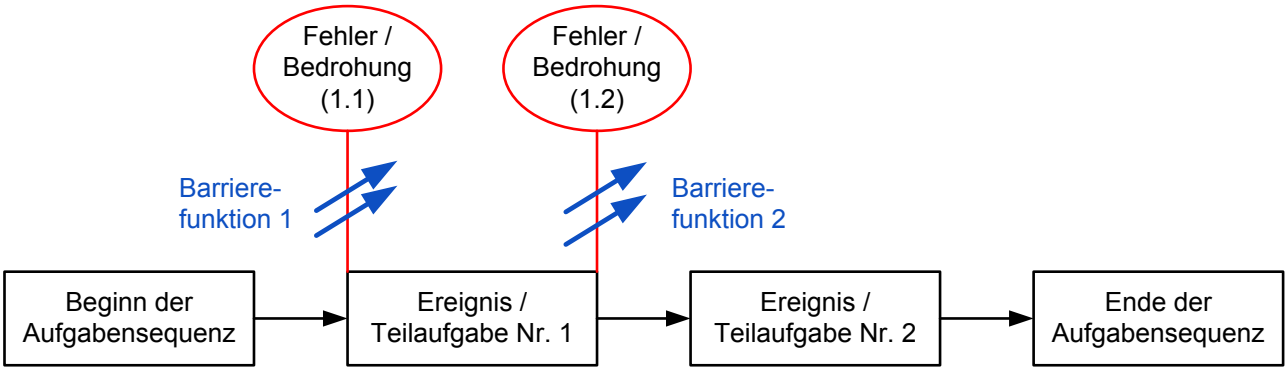

Abbildung 4.7: Event and Barrier Function Model (EBFM) nach Kecklund et al. [KEWS96] (Beispiel)

Vor- und Nachteile des Event and Barrier Function Model:

Das EBFM ist gut geeignet zur Modellierung linearer Prozesse, die in einer Sequenz ablaufen. Dabei kann das Modell flexibel auf verschiedenen Detaillierungsebenen erstellt werden. Die Darstellung ist einfach und die einzelnen Aufgaben und Abläufe lassen sich intuitiv richtig nachvollziehen. Wirken ein Fehler oder eine Barrierefunktion auf zwei Teilaufgaben, werden sie doppelt gezeichnet, also wiederholt. Das kann dazu führen, dass der Leser auf den ersten Blick den Eindruck hat, es seien mehr Fehler oder Barrieren vorhanden als es tatsächlich sind. Ein bedeutender Nachteil des EBFM ist, dass in der Darstellung zwar Fehler und Barrieren, aber keine Folgen oder Gefährdungen enthalten sind.

4.9 Accident Evolution and Barrier function model

Das *Accident Evolution and Barrier function model (AEB-Modell)* [Sve91] ist ein Modell zur Beschreibung des Verlaufs von Unfällen / Vorfällen und der Ereignisse, die ihnen vorausgehen. Die Darstellung erfolgt in Form eines Ablaufdiagramms von oben nach unten (Abbildung 4.8). Der Fokus dieser Darstellung liegt auf der Interaktion zwischen Mensch und Technik und hebt potenziell gefährliche Sequenzen hervor. Ein AEB-Diagramm stellt immer eine Sequenz dar, die aus Interaktionen zwischen Mensch und Technik besteht und am Ende zu einem Unfall oder Vorfall führt. Fehlerhafte Zustände oder Funktionen werden durch Kästen dargestellt, die in zwei Spalten angeordnet werden: eine für Human Factors, bezeichnet mit HO 1 bis HO n, und eine für technische Systeme, bezeichnet mit T 1 bis T m. Pfeile zwischen diesen Kästen stellen den (ungefähren) zeitlichen Ablauf der Ereignisse dar, aber nicht notwendigerweise die kausalen Zusammenhänge. An diesen Pfeilen sind Barrierefunktionen (//1 bis //x) angetragen, die den Unfallverlauf hätten stoppen können oder ihn gestoppt haben.

[4] Das Modell von Kecklund [KEWS96] ist ursprünglich schwarz-weiß. Die Farben wurden hier zum besseren Verständnis hinzugefügt.

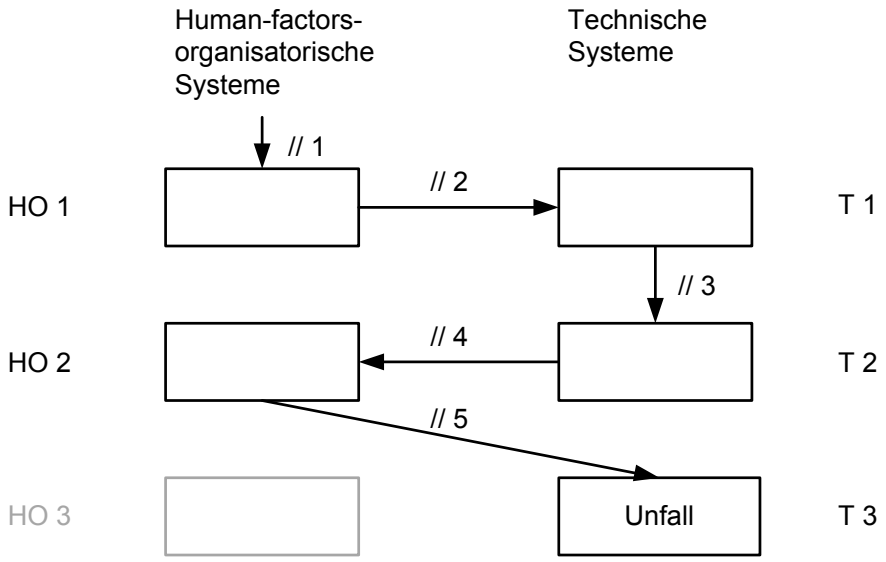

Abbildung 4.8: AEB-Diagramm nach Svenson [Sve91] (Beispiel)

Vor- und Nachteile des Accident Evolution and Barrier function model:

Das AEB-Modell beschreibt die zeitliche Reihenfolge der Ereignisse. Dabei beschränkt es sich auf eine einzelne, als wesentlich eingestufte Ursache bzw. ein wesentliches Ereignis und stellt die Ereigniskette von dort aus dar. Bei der Interpretation des AEB-Diagramms muss beachtet werden, dass die Pfeile im Diagramm nicht immer kausale Zusammenhänge beschreiben. Sie beschreiben den zeitlichen Ablauf, der nicht immer auch der direkten Ursache-Wirkungs-Beziehung entspricht. Dadurch wird die Bestimmung von geeigneten Vermeidungsmaßnahmen erschwert. Insgesamt ist die Darstellung jedoch einfach, verständlich und intuitiv richtig zu interpretieren.
Ein AEB-Diagramm kann flexibel auf verschiedenen Detaillierungsebenen eingesetzt werden. Dabei entscheidet die Art der Modellierung eines Fehlers (als Kasten oder als Versagen einer Barrierefunktion) über die Detaillierungsebene.
Laut Svenson [Sve91] kann das AEB-Modell auch im Rahmen einer präventiven Sicherheitsanalyse verwendet werden. Bislang wurde es jedoch vor allem im Rahmen der Analyse von Unfällen oder Vorfällen angewendet. Aufgrund der Tatsache, dass im AEB-Modell ein ganz bestimmter zeitlicher Ablauf von Ereignissen dargestellt wird, erscheint das Modell für die Anwendung in präventiven Analysen als nur bedingt geeignet.

4.10 Sicherheitsbarrierendiagramm

Das *Sicherheitsbarrierendiagramm (SBD)* [Dui09] ist ein gerichteter bipartiter Graph, dessen Knoten Zustände (oder Ereignisse) und Barrieren darstellen (Abbildung 4.9). Es wird von links nach rechts gelesen und beschreibt eine Entwicklung von einem oder mehreren Ausgangszuständen oder -ereignissen zu einer oder mehreren Folgen. Diese Entwicklung wird kausal beschrieben und beinhaltet daher auch einer grobe zeitliche Darstellung. Der Zustand / das Ereignis links von einer Barriere beansprucht (aktiviert) diese Barriere. Versagt die Barriere, tritt der Zustand / das Ereignis auf der rechten Seite der Barriere ein. Pfeile verdeutlichen diesen Zusammenhang.
Das Diagramm kann sich an einer Barriere verzweigen (divergieren, z. B. an Barriere B5 in Abbildung 4.9): Zusätzlich zum Zustand nach dem Versagen einer Barriere können rechts von der Barriere noch weitere Zustände abgebildet werden, z. B. Zustände nach erfolgreichem Einsatz der Barriere. Im Diagramm können auch zwei Pfade zusammengeführt werden (konvergieren, z. B. an den Barrieren B1 und B2): Dann kann ein Zustand auf zwei verschiedenen Pfaden erreicht werden (logisches

ODER). Das Diagramm kann sich in einem Zustand verzweigen (z. B. am Zwischenereignis 1): Versagt eine Barriere auf der linken Seite dieses Zustands, werden beide Barrieren auf der rechten Seite beansprucht, um die Folgen abzuwenden (logisches UND). Es können auch explizit UND- und ODER-Gatter in das Diagramm eingefügt werden.
Das SBD wird vor allem präventiv im Rahmen einer Risikoanalyse eingesetzt. Da es mögliche Unfallszenarien darstellt, kann es auch zur Darstellung von Unfallabläufen eingesetzt werden. Für die Konstruktion eines SBD gibt es strenge Regeln, z. B. darf eine Barriere nicht durch einen parallelen Pfad ohne Barriere umgangen werden [Dui09].

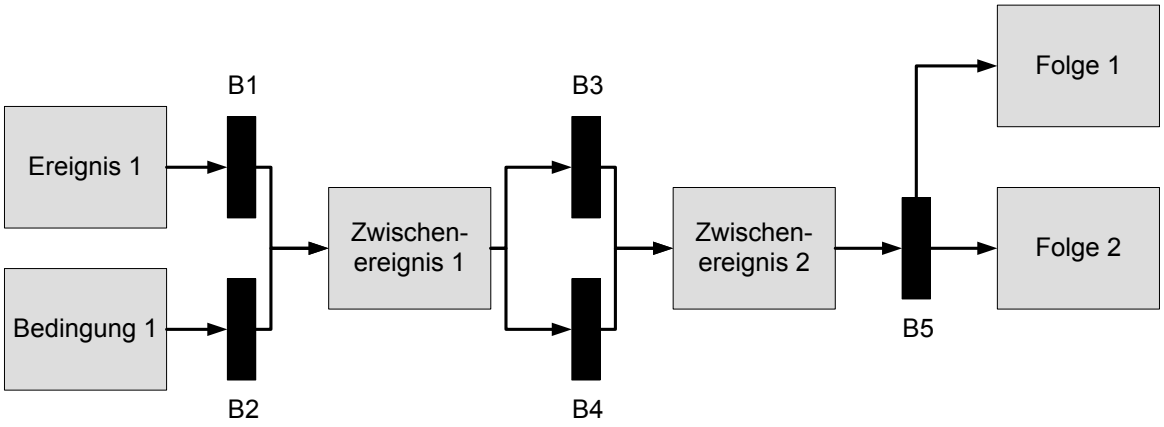

Abbildung 4.9: Sicherheitsbarrierendiagramm nach Duijm [Dui09] (Beispiel)

Vor- und Nachteile des Sicherheitsbarrierendiagramms:

Das Sicherheitsbarrierendiagramm (SBD) lässt sich flexibel auf verschiedenen Detaillierungsebenen einsetzen. Im Vergleich zu anderen Darstellungsweisen ist das SBD allerdings deutlich komplexer. Die Darstellung ist zudem nicht immer intuitiv richtig zu interpretieren. Dies betrifft vor allem das Verzweigen und Zusammenführen von Pfaden. Dem Betrachter erschließt sich dabei nicht immer sofort die Bedeutung: Handelt es sich um alternative Möglichkeiten? Sind es UND- oder ODER-Verknüpfungen? Hier muss dem Betrachter die Darstellung erläutert werden.

4.11 Barriereblockdiagramm

Ein *Barriereblockdiagramm (BBD)* [SH04] dient der Darstellung von im System verfügbaren Barrierefunktionen. Die Aufgabe dieser Barrierefunktionen ist es zu verhindern, dass ein Prozess oder ein System aufgrund eines bestimmten auslösenden Ereignisses eskaliert. Ein BBD besteht aus einem auslösenden Ereignis, einer oder mehreren Barrierefunktionen, möglichen Folgen und Pfeilen, die die Ereignissequenz darstellen (Abbildung 4.10). Erfüllt eine Barriere ihre Funktion, so wird der Pfeil waagerecht von der Barrierefunktion nach rechts gezeichnet. Ein Pfeil nach unten bedeutet, dass die Barriere versagt. Ähnlich wie beim SBD ist die Beschreibung der Ereignisse im BBD kausal und beinhaltet daher auch eine grobe zeitliche Darstellung.

Vor- und Nachteile des Barriereblockdiagramms:

Das Barriereblockdiagramm ist im Gegensatz zum Sicherheitsbarrierendiagramm deutlich intuitiver und einfacher zu erstellen. Diese Vorteile rühren vor allem daher, dass sich das BBD auf ein auslösendes Ereignis und die daraus möglicherweise erwachsenden Folgen konzentriert. Es stellt also nur einen kleinen Ausschnitt aus einem komplexen System oder Prozess dar. Dabei kann der Analyst

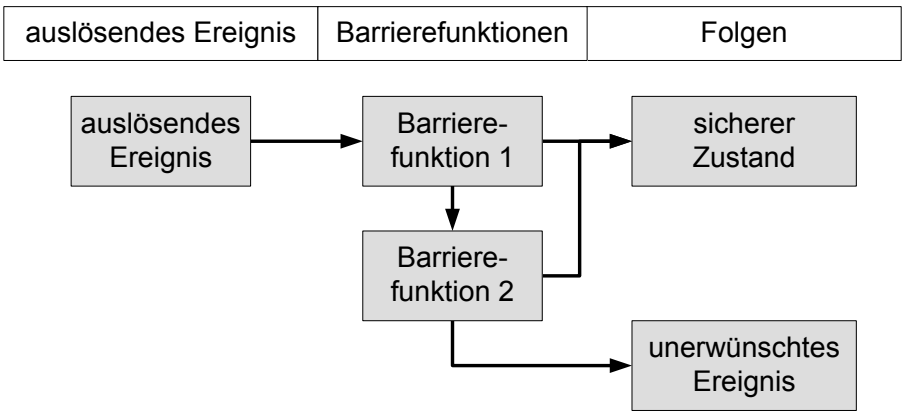

Abbildung 4.10: Barriereblockdiagramm nach Sklet et al. [SH04] (Beispiel)

die Detaillierungsebenen flexibel nach seinen Bedürfnissen wählen. Das Anwendungsgebiet des BBD ist vor allem die präventive Analyse. Dadurch, dass in einem BBD nur ein kleiner Ausschnitt eines Systems dargestellt wird, ist die Möglichkeit zur Darstellung von Unfallhergängen mittels BBD stark eingeschränkt.

4.12 Vergleich der Darstellungsweisen

Tabelle 4.1 zeigt in einem Vergleich, inwiefern die oben beschriebenen Modelle und Darstellungsweisen die Anforderungen D-1 bis D-11 erfüllen. Die Tabelle dient als Basis für die Auswahl einer geeigneten Darstellungsweise für Sicherheitsschichten. Für die Bewertung werden die folgenden drei Kategorien verwendet:

\+ ja / sehr
o eingeschränkt / möglich / mittel
\- nein / wenig / nicht dazu gedacht

Wo eine Bewertung mit diesen drei Kategorien nicht ausreichend ist, erfolgt die Bewertung in Textform. Zusätzlich zu den Anforderungen D-1 bis D-11 wird untersucht, worauf das Denken des Betrachters gelenkt wird und wie hoch der Formalisierungsgrad des Modells bzw. der Darstellungsweise ist. Ein hoher Formalisierungsgrad erhöht die Wahrscheinlichkeit dafür, dass zwei verschiedene Analysten das Modell auf die gleiche Weise erstellen würden. Verschiedene Modelle werden dadurch vergleichbarer und auch die Prüfung des Modells auf Korrektheit wird erleichtert. Für die Bewertung des Formalisierungsgrads werden folgende Kategorien verwendet:

\+ Der Zeichenvorrat und die Art der Modellierung (d. h. die Art, wie das Diagramm aufgebaut wird) sind formal definiert.
\- Keine Formalisierung. Das Vorhandensein eines minimalen Formalisierungsmerkmals, wie z. B. der eindeutig dargestellten Anzahl der Sicherheitsschichten, wird hierbei nicht als ausreichendes Kriterium für eine Formalisierung gewertet.

Die Auswahl des besten Modells bzw. der besten Darstellungsweise erfolgt unter Zuhilfenahme der Bewertung aus Tabelle 4.1. Zusätzlich wird berücksichtigt, wie wichtig die Erfüllung der einzelnen Anforderungen D-1 bis D-11 sowie der weiteren Kriterien im Hinblick auf das Ziel der vorliegenden Arbeit ist.
Die meisten hier beschriebenen Darstellungsweisen sind intuitiv richtig zu interpretieren. Beinahe alle erlauben es, explizit Barrieren oder ähnliche Elemente darzustellen. Das einzige Modell, in dem keine Barrieren dargestellt werden können, ist das *Dominomodell*. Daher ist es zur Darstellung von

Tabelle 4.1: Vergleich der verschiedenen Modelle und Darstellungsweisen sowie Auswahl des für den Zweck der vorliegenden Arbeit am besten geeigneten Modells, wie im Text erläutert

Modell / Darstellungsweise	einfach (D-1)	intuitiv (D-2)	flexibel (D-3)	verschiedene Systemelemente (D-4)	Barrieren / Sicherheitsmaßnahmen (D-5)	zeitlich (D-6)	kausal (D-7)	Ursachen (D-8)	End-Folgen (D-9)	Unfall (D-10)	präventiv (D-11)	Formalisierung	lenkt Denken auf
Energiemodell	+	+	o	o	+	-	-	eine	keine explizit	o	+	-	Energie
ZSM	+	+	o	+	+	+	+	je eine	keine explizit	-	+	-	Eskalationsstufen
LOPA-Diagramm	+	o	o	o	+	+	+	je eine	eine	-	+	+	USE
Dominomodell	+	-	-	-	-	+	+	je eine	eine	+	-	-	Mensch
SCM	o	+	+	+	+	-	+	mehrere	eine	+	+	-	Barrieren, Lücken
Fliegendiagramm	o	+	+	+	+	o	+	mehrere	mehrere	+	+	-	zentrales Ereignis, Ursachen, Folgen
EBFM	+	+	+	+	+	+	+	mehrere	keine explizit	o	+	+	Prozessschritte, Barrieren
AEB-Diagramm	+	+	+	+	+	+	-	keine kausale	eine	+	o	+	Interaktion Mensch – Technik
SBD	-	-	+	+	+	o	+	mehrere	mehrere	+	+	+	Barrieren
BBD	+	+	+	+	+	o	+	eine	mehrere	-	+	+	Barrieren

Sicherheitsschichten ungeeignet. Die Darstellungsweisen im unteren Bereich der Tabelle 4.1 sind auf verschiedenen Detaillierungsebenen flexibel einsetzbar und erlauben es, alle Arten von Systemelementen darzustellen, z. B. technische, menschliche und organisatorische. Diese Eigenschaften sind sehr wichtig für die Darstellung von Sicherheitsschichten, sodass das *Energiemodell*, das *Zwiebelschalenmodell (ZSM)* und das *LOPA-Diagramm*, die hier Schwächen haben, ebenfalls als Darstellungsweise ausscheiden.
Für Anwendungen zur Sicherheitsbetrachtung und zum Sicherheitsnachweis ist eine Berücksichtigung der kausalen Zusammenhänge wichtiger als die zeitliche Abfolge der Ereignisse. Dadurch ist das *AEB-Diagramm* für den Zweck der vorliegenden Arbeit weniger gut geeignet. Zudem eignet sich das AEB-Diagramm nur bedingt zum Einsatz in präventiven Analysen.
Das *Event and Barrier Function Model (EBFM)* stellt die Folge(n) des Versagens der Sicherheitsmaßnahmen nicht explizit dar, da es sich an einer Aufgabensequenz orientiert. Dies entspricht nicht dem im Eisenbahnbereich üblichen Vorgehen, die Sicherheit eines Systems im Hinblick auf bestimmte Gefährdungen zu betrachten. Das *Barriereblockdiagramm (BBD)* erfüllt zwar viele der Kriterien für eine gute Darstellungsweise, stellt aber nur einen kleinen Ausschnitt des Systems dar. Dies wird auch dadurch deutlich, dass es nur eine Ursache darstellt. Daher ist es für den Zweck der vorliegenden Arbeit ebenfalls nicht geeignet.
Die drei verbleibenden Darstellungsweisen, das Schweizer-Käse-Modell (SCM), das Fliegendiagramm und das Sicherheitsbarrierendiagramm (SBD), sind prinzipiell für den Zweck der vorliegenden Arbeit geeignet. Das *Sicherheitsbarrierendiagramm* hat einen hohen Formalisierungsgrad, ist jedoch deutlich komplexer als die anderen Darstellungsweisen und vor allem nicht immer intuitiv richtig zu interpretieren.
Das *Fliegendiagramm* betrachtet neben den Ursachen auch verschiedene mögliche Folgen eines unerwünschten Ereignisses. Im Rahmen der vorliegenden Arbeit soll jedoch der Schwerpunkt auf Maßnahmen zum Verhindern eines unerwünschten Ereignisses liegen. Schadensbegrenzende Maßnahmen werden nicht betrachtet. Im Eisenbahnsystem führt große kinetische Energie zusammen mit langen Bremswegen der Züge dazu, dass der potenzielle Schaden meist sehr groß ist und eine Schadensbegrenzung kaum möglich erscheint[5]. Das Fliegendiagramm stellt somit einen Bereich dar, der bei Analysen im Eisenbahnbereich häufig nicht benötigt wird, und soll daher zur Darstellung von Sicherheitsschichten nicht verwendet werden.
Von den untersuchten Darstellungsweisen ist das **Schweizer-Käse-Modell (SCM)** am besten zur Darstellung von Sicherheitsschichten geeignet. Es ist intuitiv, flexibel und präventiv anwendbar. Es erlaubt es, verschiedenste Systemelemente in Form von Sicherheitsschichten darzustellen und ist dabei auf eine Folge / einen Unfall bezogen. Wird als Folge eine Gefährdung statt eines Unfalls gewählt, so entspricht das Modell den Bedürfnissen der im Eisenbahnbereich üblichen Form der Sicherheitsbetrachtung. Die Darstellung der Sicherheitsschichten eines Systems dient nicht der Systementwicklung oder der Automatisierung der Implementierung des Systems (siehe [Sch99]). Vielmehr handelt es sich um eine erläuternde Darstellung der Sicherheitsschichten zum besseren Verständnis der im System vorhandenen Sicherheitsmaßnahmen – ohne Reihenfolgeabhängigkeit (siehe Anforderung S-14, Abschnitt 3.1). Daher kann der geringe Formalisierungsgrad des SCM für den Einsatz zur Darstellung von Sicherheitsschichten toleriert werden. Ein besonderer Vorteil des SCM gegenüber allen anderen Darstellungsweisen ist die explizite Darstellung von Lücken in den Barrieren. Diese Betonung der Tatsache, dass Sicherheitsmaßnahmen niemals 100%igen Schutz bieten, ist für die Modellierung von Sicherheitsschichten ein großer Vorteil.

[5] Eine Ausnahme hierbei sind Brände, bei denen Maßnahmen zur Schadensbegrenzung in Form der Brandbekämpfung eine wichtige Rolle spielen.

5 Vorhandene Methoden

Heutzutage ist eine große Zahl sicherheitsrelevanter Systeme in verschiedenen Domänen in Betrieb, und ihre Zahl nimmt stetig zu. Alle diese Systeme enthalten Sicherheitsmaßnahmen zur Beherrschung von Gefährdungen. In der zugehörigen Systemdokumentation (Entwurfsdokumente, Handbücher, ...) sind jedoch – insbesondere im Bereich der Eisenbahn – nur in wenigen Fällen die im System enthaltenen Sicherheitsmaßnahmen explizit beschrieben. Das bedeutet, in vielen Fällen ist nicht explizit dokumentiert, welche Sicherheitsmaßnahmen in einem System enthalten sind. Daher bedarf es einer *Methode*, um in bereits bestehenden Systemen die vorhandenen Sicherheitsschichten zu identifizieren.

Eine Methode ist „ein nach Gegenstand und Ziel planmäßiges (methodisches) Verfahren, die Kunstfertigkeit einer Technik zur Lösung praktischer und theoretischer Aufgaben“[1] [Bro06]. Eine Methode hat stets einen Zweck, z. B. die Lösung einer mathematischen Gleichung. Eine Methode beinhaltet stets eine Anleitung, wie zur Erlangung der Ergebnisse vorzugehen ist. Je detaillierter diese Anleitung ist, desto leichter ist die Methode anzuwenden und desto reproduzierbarer sind ihre Ergebnisse.

Da der Begriff Sicherheitsschicht in Abschnitt 3.2 neu definiert wurde, ist nicht zu erwarten, dass bereits Methoden zur expliziten Identifikation von Sicherheitsschichten existieren. Daher wird an dieser Stelle nicht nur nach einer Methode zur Identifikation von Sicherheitsschichten gesucht. Stattdessen werden Methoden zusammengetragen, die Sicherheitsmaßnahmen identifizieren. Dabei werden insbesondere solche Methoden aufgeführt, die Barrieren oder Barrierefunktionen identifizieren, denn diese können Bestandteile von Sicherheitsschichten sein (siehe Abschnitt 3.2). Da in verschiedenen Domänen ähnliche Konzepte verwendet werden, aber die verwendeten Begriffe unterschiedlich sind (siehe Kapitel 2), werden darüber hinaus auch Methoden betrachtet, die Sicherheitsfunktionen, Schutzebenen und ähnliche Sicherheitsmaßnahmen identifizieren oder analysieren.

In den folgenden Abschnitten werden zunächst die Anforderungen an die gesuchte Methode definiert. Anschließend wird ein Überblick über einige ausgewählte, vielversprechende klassische Methoden aus der Literatur gegeben. Die Auswahl der Methoden erfolgt unabhängig davon, welches Modell und welche Darstellungsweise (Beschreibungsmittel) sie nutzen. Auch wenn das von der Methode verwendete Modell oder die Darstellungsweise in Abschnitt 4.12 als ungeeignet eingestuft wurde, so kann die Methode doch Schritte enthalten, die zur Identifikation von Sicherheitsschichten oder ihrer Bestandteile Barriere und Barrierefunktion geeignet sind. Zu jeder Methode werden die wichtigsten Vor- und Nachteile, insbesondere im Hinblick auf die Zielsetzung der vorliegenden Arbeit, diskutiert. Anschließend werden die Methoden miteinander verglichen, und auf Grundlage der definierten Anforderungen wird entschieden, welche Methode zur Identifikation von Sicherheitsschichten am besten geeignet ist.

[1] Die im Zitat ursprünglich verwendeten Abkürzungen wurden von der Autorin ausgeschrieben, um eine bessere Lesbarkeit zu erreichen.

5.1 Anforderungen an die gesuchte Methode

Für den Zweck der vorliegenden Arbeit wird eine Methode benötigt, die Folgendes leisten kann:

- M-1 Die Methode soll Sicherheitsmaßnahmen bzw. Sicherheitsschichten identifizieren.
- M-2 Die Methode soll eine Basis für eine quantitative Bewertung der Sicherheitsmaßnahmen bzw. Sicherheitsschichten bereitstellen, um so die Anforderungen nach einer quantitativen Risikobetrachtung (Gefährdungsraten) der DIN EN 50129 [DIN03] erfüllen zu können.

Anmerkung: Für die vorliegende Arbeit von besonderer Bedeutung sind Methoden zur *Identifikation* von Sicherheitsschichten (M-1). Die *Quantifizierung* ist der darauf aufsetzende zweite Schritt. Falls keine geeignete Methode für eine quantitative Bewertung vorhanden ist, kann zunächst auf eine qualitative Bewertung zurückgegriffen werden.
Weitere Anforderungen an die gesuchte Methode sind:

- M-3 Die Methode soll für den Bahnbereich anwendbar sein.
- M-4 Die Methode soll geeignet sein, um ein generisches Modell der Sicherheitsschichten des Systems zu erzeugen (nicht nur ein anlagenspezifisches).
- M-5 Die Ergebnisse der Methode sollen für die Sicherheitsnachweisführung weiterzuverwenden sein. Insbesondere ist hier der Abschnitt 3 (Ausfallauswirkungen) des technischen Sicherheitsberichts gemäß DIN EN 50129 [DIN03] zu berücksichtigen.
- M-6 Die Methode soll alle Arten von Systemelementen behandeln können. Sie soll für technische Systeme geeignet sein, aber auch Raum für menschliche Einflüsse und Handlungen bieten sowie organisatorische Aspekte zulassen.
- M-7 Die Methode soll möglichst leicht zu erlernen sein, oder aber auf einer (evtl. schwierigen) Standard-Methode aus dem Eisenbahnbereich aufsetzen.
- M-8 Die Ergebnisse der Methode sollen in Form eines Modells graphisch darstellbar sein.
- M-9 Die Methode soll präventiv, d. h. bereits vor einem Unfall, anwendbar sein.
- M-10 Die Methode soll Fehler- / Ausfallkombinationen berücksichtigen, denn 1-Fehler-Sicherheit ist in vielen Teilbereichen des Eisenbahnsystems bereits Standard.
- M-11 Die Methode soll einen deduktiven Anteil haben, um den Anforderungen der DIN EN 50129 [DIN03] bzgl. der Betrachtung von Ausfällen nachzukommen.
- M-12 Die Methode soll einen induktiven Anteil haben, um die deduktive Analyse gemäß den Empfehlungen der DIN EN 50129 [DIN03] zu unterstützen.

5.2 Methoden im Überblick

In der Literatur gibt es zahlreiche Texte über Modelle und Darstellungsweisen, die Sicherheitsmaßnahmen beinhalten (siehe auch Kapitel 4). In den Kurzfassungen dieser Texte werden oft (neue) Methoden zur Analyse von Sicherheitsmaßnahmen angepriesen.

5.2.1 Methoden zur Unfallanalyse

Eine Möglichkeit zur Identifikation von Sicherheitsmaßnahmen, insbesondere von Barrieren, sind *Unfall-(Ursachen-)Analysen*. Methoden zur Unfallanalyse zielen darauf ab, aus Unfällen zu lernen. Voraussetzung für eine solche Analyse ist eine erste Beschreibung des Unfallhergangs. Einen Überblick über Methoden zur Unfallanalyse gibt z. B. Sklet in [Skl02]. Einige dieser Methoden nutzen das Konzept von Barrieren zur Erklärung des Unfallhergangs, z. B. *Management Oversight and Risk Tree (MORT)* [FKKS02] und die *Accident Evolution and Barrier function (AEB)-Methode* [Sve91]. Die Identifikation von Barrieren erfolgt jedoch in der Regel eher „ad hoc“ [Hol99]. Bei dieser „ad

hoc"-Identifikation werden vor allem solche Barrieren identifiziert, die im untersuchten Unfall sichtbar versagt haben. Sie sind relativ leicht zu identifizieren, denn ihr Versagen ist Teil des Unfallhergangs. Das Versagen der Barrieren wird meist über einen Vergleich zwischen dem Soll-Ablauf und dem tatsächlichen Ablauf der Ereignisse erkannt. Gängige Techniken sind z. B. das Markieren von entsprechenden Textpassagen in Unfallberichten mit Textmarkern oder Interviews, in denen Personen, die mit dem System vertraut sind, gefragt werden, wie das System hätte reagieren sollen. Das identifizierte Systemelement, das versagt hat, wird dann als „Barriere" bezeichnet. Dabei wird oft nur rudimentär geprüft, wie stark der Einfluss dieser „Barriere" auf den Unfallhergang tatsächlich war oder in Zukunft sein wird (Wäre der Unfall auch geschehen, wenn diese Barriere nicht versagt hätte?). Viele Methoden geben dem Analysten hier keine strengen Prüfkriterien an die Hand. Eine positive Ausnahme hiervon bildet die *Why-Because-Analyse (WBA)* [Lad99].
Methoden zur Unfallanalyse haben in der Regel eine *eingeschränkte Sicht auf das System*, denn sie dienen dazu, einen bestimmten Unfall zu analysieren und seine Wiederholung zu vermeiden. Sie untersuchen daher in der Regel nicht das gesamte System, sondern nur die Teile, in denen unerwünschte Ereignisse auftraten. Für den Zweck der vorliegenden Arbeit genügt es jedoch nicht, Sicherheitsmaßnahmen allein durch die Analysen von Unfällen zu identifizieren. Unfälle geschehen im Eisenbahnsystem glücklicherweise selten, daher sind Unfallanalysen zur Identifikation von Sicherheitsmaßnahmen nur eingeschränkt geeignet. Sicherheitsmaßnahmen müssen identifiziert werden, bevor es zu einem dieser seltenen Unfälle kommt. Aus diesem Grund werden bei der folgenden Untersuchung von vorhandenen Methoden nur einige ausgewählte Methoden zur Unfallursachenanalyse berücksichtigt.

5.2.2 Andere Methoden

Auch außerhalb von Unfallanalysen werden Sicherheitsmaßnahmen oftmals „ad hoc" identifiziert. Dazu werden z. B. in Brainstorming-Sitzungen zur ersten Abschätzung von Risiken Mechanismen genannt, die verhindern, dass ein (einzelner) Fehler im System zu einer Gefährdung wird. Typische Zitate sind:

- „Wenn dieses Bauteil ausfällt, kann nichts passieren, denn dann wird sofort eine Zwangsbremsung ausgelöst."
- „Diesen Fehler können wir selbst nicht beherrschen, aber wir schreiben eine Anweisung ins Bedienerhandbuch, dass der Triebfahrzeugführer darauf achten muss, dass . . . "
- „Wenn dieses Bauteil ausfällt, ist das nicht gefährlich, denn diesen Fehler können wir erkennen und melden und dann kann das übergeordnete System / der Bediener geeignete Maßnahmen ergreifen."

Diese genannten Mechanismen werden dann umgangssprachlich gern als Barrieren bezeichnet, ohne dass diesem Begriff eine klare Definition zugrunde liegt.
Harms-Ringdahl gibt in [HR01] einen Überblick über zahlreiche Methoden aus dem Bereich der Sicherheitsanalyse. Unter diesen Methoden sind auch einige, die für die Analyse von Sicherheitsmaßnahmen verwendet werden können. Die dort aufgeführten Methoden, die laut Harms-Ringdahl [HR01] speziell für die Analyse von Barrieren bzw. Sicherheitsfunktionen entwickelt wurden, sind:

- Sicherheitsbarrierendiagramme,
- Structured Analysis and Design Technique (SADT),
- MORT,
- AEB-Methode
- Sicherheitsfunktionsanalyse (SFA)

Diese Auffassung von Harms-Ringdahl wird im Folgenden zunächst hinterfragt, um zu entscheiden, für welche der genannten Methoden eine genauere Betrachtung im Hinblick auf das Ziel der vorliegenden Arbeit lohnenswert erscheint. *Sicherheitsbarrierendiagramme* sind eine Darstellungsweise, aber keine Methode zur Identifikation von Sicherheitsmaßnahmen (siehe Abschnitt 4.10). Die einzige

methodische Hilfestellung, die Harms-Ringdahl zur Identifikation der dargestellten Sicherheitsbarrieren gibt, ist, von Energiequellen auszugehen und in deren Umgebung nach Barrieren zu suchen. Dies ist als Methode nicht ausreichend. *SADT* ist eine Methode aus dem Bereich der Softwareentwicklung, die laut Harms-Ringdahl [HR01] auch zur Analyse von Sicherheitsmanagementsystemen verwendet werden kann. Aufgrund ihres eingeschränkten Anwendungsbereichs wird diese Methode hier nicht weiter betrachtet. *MORT* [FKKS02] ist eine Methode, in deren Fokus Managementsysteme stehen. Sie dient vor allem dazu, Unfallanalysen durchzuführen, kann laut Harms-Ringdahl [HR01] jedoch auch zur Systemanalyse verwendet werden. MORT basiert auf dem Energiemodell und daher wird die *Energy Trace and Barrier Analysis (ETBA)* als Vorbereitung von MORT genutzt [FKKS02]. MORT verwendet ein Diagramm, das einem Fehlerbaum ähnelt. Da der Fokus von MORT auf Managementsystemen liegt, soll es hier nicht weiter betrachtet werden. Jedoch werden die vorgelagerte Methode ETBA sowie die Fehlerbaumanalyse (FTA) in den folgenden Abschnitten diskutiert. Der *AEB-Methode* und *SFA* sind im Folgenden ebenfalls eigene Abschnitte gewidmet.
Neben den Methoden, die eigens für die Analyse von Barrieren und Sicherheitsfunktionen entwickelt wurden, gibt Harms-Ringdahl noch einige Methoden an, die für diesen Zweck adaptiert werden können: die Barriereanalyse, die Ereignisbaumanalyse (ETA) und die bereits erwähnte FTA. Sie werden ebenfalls auf ihre Eignung zur Identifikation von Sicherheitsschichten hin untersucht.

5.3 Why-Because-Analyse

Die *Why-Because-Analyse (WBA)* [Lad99] ist eine Methode zur Unfallursachenanalyse. Zu Beginn der Analyse wird zunächst das zu untersuchende Ereignis klar definiert. Dabei kommen im Rahmen einer Unfalluntersuchung durchaus mehrere Ereignisse in Frage, z. B. „Zug entgleist“ oder „Drei Tote bei Entgleisung“. Die Ergebnisse von Why-Because-Analysen der beiden genannten Ereignisse sehen unterschiedlich aus.
Eine WBA besteht aus zwei Teilen: der Why-Because-Graph-Methode und der Verifikation.

5.3.1 Why-Because-Graph-Methode

Bei der Why-Because-Graph-Methode wird ein Why-Because-Graph (WBG) erstellt, der die Ursachen für das zu untersuchende Ereignis enthält und diese in eine kausale Beziehung bringt. Die Basis bildet in der Regel ein Unfallbericht. Die Methode kann aber auch bereits zur Erstellung eines Unfallberichts unterstützend angewandt werden.
Zunächst werden alle signifikanten Ereignisse und Zustände aufgelistet, die zum Unfall beigetragen haben oder im Verlauf des Geschehens eine Rolle gespielt haben. Sie bilden die Knoten des WBG (Abbildung 5.1). Es wird zwischen vier Arten von Knoten unterschieden: Zustand, Ereignis, Prozess und Nicht-Ereignis.
Im nächsten Schritt werden die kausalen Relationen (Ursache – Folge) zwischen allen aufgelisteten Punkten bestimmt. Die Punkte werden dann als Graph in einer Baum-ähnlichen Struktur dargestellt. Das zu untersuchende Ereignis bildet die Wurzel des Baums und wird oben an der Spitze des Graphen dargestellt. Unter dem Ereignis werden die Ursachen, die zu seinem Eintritt geführt haben, abgebildet. Die Kanten des Graphen sind von den Ursachen zu den Folgen gerichtet und bilden die kausale Struktur der Geschehnisse ab. Dabei sind die Kinder eines Knoten seine direkten Ursachen, seine sogenannten *kausalen Faktoren*. Um die kausalen Faktoren zu bestimmen, wird mit den in Frage kommenden Kandidaten aus den aufgelisteten Punkten der *Counterfactual Test* durchgeführt: B ist ein kausaler Faktor von A, wenn gilt: Wenn B nicht eingetreten wäre, dann wäre auch *A* nicht eingetreten. Dabei bewegt sich der Analyst gedanklich in der „nächstmöglichen Welt“, d. h. alles außer *B* bleibt gleich.
Die Tiefe der Analyse und ihr Detaillierungsgrad werden nach Bedarf entschieden. Die Blätter des WBG, an denen der Graph endet, werden als Grundursachen bezeichnet. Sie sind ein bevorzugter

Ansatzpunkt für Verbesserungen.

5.3.2 Verifikation

Der zweite Teil der WBA, die Verifikation, ist ein formaler Beweis dafür, dass die kausalen Relationen im WBG korrekt sind und hinreichend viele kausale Faktoren für jeden Knoten (mit Ausnahme der Blätter) gefunden wurden. Zu diesem Zweck wird auf die kausalen Faktoren im WBG der *Causal Completeness Test* angewendet. Hierbei wird geprüft, ob bei Eintreten aller kausalen Faktoren eines Knotens A, auch A zwingend eintreten muss.
Die Verifikation ist ein optionaler Teil der WBA. Sie ist nur für fortgeschrittene, sichere Anwender der WBG-Methode geeignet. Aufgrund der strengen Logik hat ein WBG die Eigenschaft, dass der Unfall so nicht stattgefunden hätte (und so kein zweites Mal stattfinden kann), wenn ein beliebiger kausaler Faktor aus dem Graph / dem Geschehen entfernt wird.

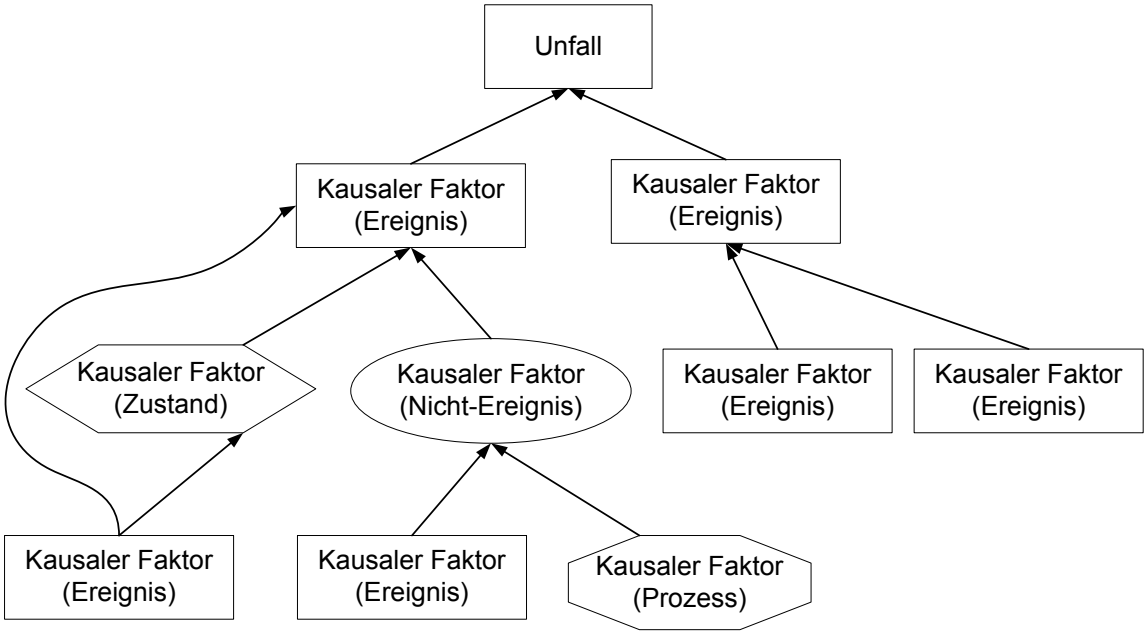

Abbildung 5.1: Why-Because-Graph in der Notation nach Sanders [SanoJ]

5.3.3 Vor- und Nachteile der Why-Because-Analyse

Die WBA ist zur Analyse und Darstellung von Unfällen in komplexen Systemen geeignet und kann dabei sowohl technische als auch organisatorische Aspekte sowie menschliche Handlungen und sogar Umgebungsbedingungen berücksichtigen. Sie wurde zur Analyse von Eisenbahn-Unfällen bereits erfolgreich eingesetzt, siehe z. B. [Lem05, Sch05].
Ein großer Vorteil der WBA besteht darin, dass sie sicherstellt, dass alle wichtigen Ursachen für den Unfall identifiziert werden. Hierdurch wird eine wesentliche Schwäche klassischer Unfallanalysen vermieden: Das Konzentrieren auf nur eine Grundursache, das mitunter zu voreiligen Schuldzuweisungen führen kann. Die Darstellung des WBG ist auch für Nicht-Experten leicht verständlich. Allerdings ist die Anwendung der beiden logischen Tests nicht ganz einfach und erfordert einige Übung.
Ein interessanter Aspekt der WBA ist, dass sie im Gegensatz zu den meisten anderen Unfallanalysemethoden nicht nur Ausfälle, Versagen und Fehlhandlungen identifiziert, sondern auch korrekt[2]

[2]Korrekt bedeutet in diesem Zusammenhang, dass die Funktionen, Handlungen etc. so ausgeführt wurden, wie sie geplant bzw. vorgeschrieben waren. Derartige kausale Faktoren können z. B. Hinweise auf eine fehlerhafte Spezifikation sein.

ausgeführte Funktionen, Handlungen, Prozesse etc., die den Unfall begünstigt haben. Unter den kausalen Faktoren für einen Unfall sind stets auch die Sicherheitsmaßnahmen, die versagt haben. Allerdings benennt die WBA diese Sicherheitsmaßnahmen nicht als solche. Da im Rahmen der WBA darüber hinaus noch weitere, andere kausale Faktoren identifiziert werden, z. B. Wettereinflüsse, sind die Sicherheitsmaßnahmen aus den kausalen Faktoren nicht direkt zu erkennen. Daher kann die WBA zur Identifikation von Sicherheitsmaßnahmen nur unterstützend eingesetzt werden.
Für die präventive Analyse von Systemen oder Systementwürfen ist die WBA nicht geeignet, da sie keine möglichen, sondern nur die im konkreten Fall tatsächlich aufgetretenen kausalen Faktoren identifiziert. Dadurch ist die Methode für die Sicherheitsnachweisführung ungeeignet.

5.4 Sicherheitsfunktionsanalyse

Die *Sicherheitsfunktionsanalyse (SFA)* von Harms-Ringdahl [HR01] dient dazu, Sicherheitsfunktionen (SF) eines Systems zu identifizieren, zu beschreiben, zu bewerten und – falls nötig – Ansätze für Verbesserungen zu finden. Die Methode kann sowohl präventiv, d. h. zur Systemanalyse, als auch zur Untersuchung von Unfällen angewendet werden. Für den Zweck der vorliegenden Arbeit ist vor allem die präventive Anwendung interessant. SFA besteht aus sechs Schritten sowie Vor- und Nachbereitung der Analyse [HR01]:

- Vorbereitung

1. Auswahl zu untersuchender Gefährdungen
2. Identifizierung vorhandener Sicherheitsfunktionen (SF)
3. Strukturierung und Klassifizierung der SF
4. Einschätzung der Effizienz etc. der SF
5. Bewertung der SF
6. Vorschläge für Verbesserungen

- Abschluss und Bericht

Für die vorliegende Arbeit sind die Schritte 2, 4 und 5 von besonderem Interesse. Daher werden diese nachfolgend näher betrachtet.

5.4.1 Identifizierung vorhandener Sicherheitsfunktionen

Der Schritt 2 der SFA, die Identifizierung vorhandener Sicherheitsfunktionen, ist bei Harms-Ringdahl [HR01] methodisch nur kurz umrissen. Es wird auf verschiedene Ansätze hingewiesen, von denen jedoch nur zwei genauer benannt werden:

1. Das Nutzen einer strukturierten Checkliste allgemeiner Sicherheitsfunktionen
2. Durchführung von Interviews oder Gruppendiskussionen, in denen ausgehend von bestimmten Gefährdungen Fragen dazu gestellt werden, wie Wahrscheinlichkeiten und Folgen gering gehalten werden

In einer späteren Veröffentlichung von Harms-Ringdahl [HR09] zur Verwendung von SFA als Methode zur Unfallanalyse findet sich eine Kategorisierung der Möglichkeiten zur Identifizierung von Sicherheitsfunktionen:

(A) Textanalyse (Unfallberichte)
(B) Interviews
(C) Sequenzorientierte Analyse (beginnend beim Unfall rückwärts dem Lauf der Ereignisse folgend)
(D) Vergleich mit einem vorgegebenen Satz von Sicherheitsfunktionen (zur Klärung der Frage, welche dieser Sicherheitsfunktionen vorhanden waren und wie gut sie funktionierten)

Die *Textanalyse* (A) wird z. B. mit Hilfe von Textmarkern durchgeführt. Dabei werden Wörter oder Textpassagen, die einen Hinweis auf eine Sicherheitsfunktion geben, farbig markiert. Anschließend werden die gefundenen Textpassagen kopiert und in einem Protokoll vermerkt. Bei den *Interviews*

(B) werden Personen befragt, die mit dem System vertraut sind. Der Interviewer stellt dazu möglichst offene Fragen, z. B. „Was hätte den Unfall verhindern können?“. Derartige Fragen werden auch bei einer *sequenzorientierten Analyse* (C) verwendet, jedoch auch bezogen auf Ereignisse und Zustände vor dem Unfall. Der *Vergleich mit einem vorgegebenen Satz von Sicherheitsfunktionen* (D) ist im Prinzip eine Nutzung von Checklisten (siehe oben, Ansatz 1) und ist z. B. für Vergleiche zwischen mehreren untersuchten Systemen geeignet. Dieser Ansatz setzt jedoch die Existenz geeigneter Checklisten voraus.

5.4.2 Einschätzung und Bewertung der identifizierten Sicherheitsfunktionen

Ziel der Schritte 4 und 5 der SFA ist es, die Sicherheitsfunktionen bzgl. verschiedener Kriterien zu bewerten und schließlich für jede Sicherheitsfunktion zu entscheiden, ob sie akzeptabel ist oder verbessert werden muss. Kriterien können laut Harms-Ringdahl [HR10] beispielsweise die folgenden sein:

Effektivität Erfolgswahrscheinlichkeit der SF

Wichtigkeit Höhe des Einflusses der SF auf die Sicherheit

Absicht eigentlicher / hauptsächlicher Zweck der SF – Verbesserung der Sicherheit oder ein anderer, z. B. betrieblicher Zweck

Die Einschätzung erfolgt in Prozent oder in zuvor definierten Klassen und ist die Grundlage für die anschließende Bewertung. Interessant ist, dass bei dieser Vorgehensweise unter Schritt 2 möglicherweise Funktionen als Sicherheitsfunktionen identifiziert werden, die keinerlei Einfluss auf die Sicherheit des Systems haben. Das kann bei Brainstormings und ähnlichen Methoden durchaus vorkommen. Durch die Einschätzung (Schritt 4) können diese „falschen“ Sicherheitsfunktionen herausgefiltert werden.

5.4.3 Vor- und Nachteile der Sicherheitsfunktionsanalyse

Bei der SFA können sowohl technische, also auch menschliche und organisatorische Aspekte berücksichtigt werden. Die Methode wurde bereits zur Analyse eines Eisenbahnunfalls angewandt, siehe [HR09]. Die SFA beinhaltet eine Bewertung der identifizierten Sicherheitsfunktionen. Allerdings erfolgt diese Bewertung nicht quantitativ, sondern qualitativ bis semi-quantitativ.

Ein Nachteil der Methode ist, dass die Anleitung zur Durchführung der einzelnen Schritte bei Harms-Ringdahl nur sehr grob umrissen wird. Dies betrifft insbesondere Schritt 2, die Identifizierung vorhandener Sicherheitsfunktionen. Es werden hierzu nur Ansätze vorgestellt.

Die SFA konzentriert sich auf die Identifikation und Bewertung von Sicherheitsfunktionen, stellt aber keine kausalen Relationen zwischen den Systemelementen her und betrachtet auch keine Ausfallkombinationen. Daher sind ihre Ergebnisse für einen Sicherheitsnachweis (SiNa) nur eingeschränkt verwendbar.

5.5 Barriereanalyse

Die *Barriereanalyse (BA)* [Eri05], auch *Energy Trace and Barrier Analysis (ETBA)*, *Energy trace analysis* oder *Energy Analysis* genannt, ist eine Methode, um Gefährdungen im Zusammenhang mit Energiequellen zu identifizieren und zu analysieren. Mit der BA wird der ungewollte Fluss der gefährlichen Energie zu Zielen (Personen oder Gegenständen) analysiert, indem Barrieren untersucht werden, die den Energiefluss unterbinden können [Eri05]. Die BA nutzt dabei Haddons Energiemodell und die zwölf Strategien zu Gegenmaßnahmen (siehe Abschnitt 4.2). Die Methode wird vor allem präventiv zur Systemanalyse eingesetzt. Sie kann aber auch im Rahmen von Unfallanalysen unterstützend eingesetzt werden [Eri05].

Eine Barriereanalyse besteht je nach beschreibendem Autor aus bis zu zehn Schritten. Hier wird die Aufteilung von Ericson [Eri05] wiedergegeben:

1. Identifikation von Energiequellen
2. Identifikation von einfachen Energiepfaden
3. Identifikation von mehrfachen Energiepfaden
4. Identifikation von Zielen
5. Bestimmung der Verletzbarkeit der Ziele
6. Identifikation von Sicherheitsbarrieren
7. Abschätzen des Systemrisikos
8. Empfehlung von Verbesserungsmaßnahmen
9. Nachverfolgen von Gefährdungen
10. Dokumentieren der Barriereanalyse

Ein wichtiger Schritt bei einer Barriereanalyse ist Schritt 6: die Identifikation von Barrieren, die den Energiefluss zwischen der Energiequelle und dem Ziel beeinflussen können. Statt Energiequelle wird auch der Begriff *Gefährdung* verwendet. Um Barrieren zu identifizieren, sollte sich der Analyst gemäß dem Workbook des U.S. Department of Energy [U.S99] überlegen, wie die Gefährdung (die Energiequelle) und das Ziel zueinander kommen können und was benötigt wird, um Gefährdung und Ziel voneinander getrennt zu halten. Dabei wird in [U.S99] unterschieden zwischen physischen Barrieren, die

- sich direkt an der Gefährdung befinden,
- sich zwischen Gefährdung und Ziel befinden
- sich direkt am Ziel befinden

Die Identifikation von Barrieren wird durch *Checklisten* unterstützt, die mögliche Energiequellen (Tabelle 5.1) und Barrieremechanismen (Tabelle 5.2) aufführen. Zum Schritt 6 gehören auch eine Abschätzung der Auswirkungen eines Barriereausfalls sowie eine Einschätzung der Effektivität der Barrieren. Die Dokumentation der Barriereanalyse erfolgt in einem Formblatt [Eri05].

Tabelle 5.1: Auszug aus einer Checkliste für Energiequellen in Anlehnung an [Eri05]

Kategorie	**Energiequelle**
Elektrisch	Batterien, Dieselgeneratoren, Hochspannungsleitungen, in der Erde verlegte Stromleitungen, magnetische Felder, ...
Entflammbares	Chemikalien, Öl, Lösungsmittel, Verpackungsmaterial, ...
Kinetisch – linear	PKWs, LKWs, Eisenbahnen, Flugzeuge, Pressen, Projektile, Raketen, Kranladung in Bewegung, ...
Kinetisch – rotatorisch	Zentrifugen, Motoren, Ventilatoren, Bohrmaschinen, Räder, ...
Masse, Gravitation, Höhe	Treppen, Aufzüge, Gefälle, fallende Objekte, ...
Nuklear	Laboratorien, Zwischenlager, Reaktoren, Abwasserbehälter, ...
Thermisch	Hochöfen, Gasheizöfen, ausströmender Dampf, Stromleitungen, ...
...	...

5.5.1 Vor- und Nachteile der Barriereanalyse

BA ist eine leicht anzuwendende Methode, die durch die vorhandenen Checklisten gut unterstützt wird. Die identifizierten Barrieren sind jedoch ausschließlich solche, die mit Energie in Zusammenhang stehen. Auch bei diesem limitierten Anwendungsbereich kann die Benutzung der Checklisten nicht garantieren, dass alle gefährlichen Energiequellen und Barrieren identifiziert werden. Die Checklisten der BA basieren auf Haddons Arbeit [Had95], auf seinen Strategien, vor allem aber auf Erfahrung

Tabelle 5.2: Beispiel einer Checkliste für Barrieremechanismen, um gefährliche Energieflüsse zu steuern, in Anlehnung an [Eri05]

Barrieremechanismus Strategie	**Barrieremechanismus Umsetzung**
Eliminieren der Energiequelle	im Design eliminieren
Reduzieren der Energiemenge	Fahrzeuggeschwindigkeit reduzieren, schwere Güter ebenerdig lagern, Chemikalien durch weniger energetische ersetzen, Dammhöhe reduzieren, Spannung reduzieren, ...
Trennung von Energie und Ziel in Zeit und / oder Raum	betriebliche Regeln zum Abstand halten, Bedienung per Fernsteuerung, Lichtsignalanlagen installieren, durchgezogene Fahrbahnmarkierungen, ...
Isolierung durch Einfügen materieller Barrieren	Leitplanken errichten, Schutzbrillen aufsetzen, Schutzanzüge tragen, Absperrungen, Schranken, ...
Schulung von Personal zum Verhindern, dass Energie freigesetzt wird	Warnschilder, spezielle Prozeduren, Sicherheitstraining, ...
...	...

mit anderen Anlagen. Daher ist zu erwarten, dass die Anwendung auf technisch neuartige Systeme schwieriger sein wird. Für den Bereich der Eisenbahn sind noch keine angepassten Checklisten verfügbar. Eine Anwendung der BA im Eisenbahnbereich erscheint jedoch möglich und ist für Suizide im Zusammenhang mit der Eisenbahn bereits ansatzweise erfolgt (siehe [RSA08]).
Im Rahmen einer BA können alle Arten von Systemelementen als Barrieren aufgefasst werden. Auch das Versagen mehrerer Barrieren und mehrfache Energiepfade werden berücksichtigt. Allerdings entspricht dies keiner vollständigen Analyse von Mehrfachausfällen, sodass die Ergebnisse der BA im Rahmen von Sicherheitsnachweisen nur unterstützend herangezogen werden können.

5.6 Fehlerbaumanalyse

Die *Fehlerbaumanalyse (FTA)* [DIN81, DIN90a] ist eine klassische und weit verbreitete deduktive Methode, um Systeme bzgl. ihrer Ausfälle oder Fehler zu analysieren. Ziel einer FTA ist es zu ermitteln, welche Kombinationen von Ausfällen von Komponenten eines Systems zu einem bestimmten unerwünschten Ereignis führen. Ausgehend vom unerwünschten Top-Ereignis, das die Wurzel des Fehlerbaums bildet, werden mögliche Ursachen (Ausfälle von Systemkomponenten) für dieses Ereignis bestimmt. Dabei steht der Baum quasi auf dem Kopf: die Wurzel des Baums wird oben gezeichnet, die Blätter befinden sich unten. Die Ursachen werden als Knoten unter der Wurzel eingetragen und durch *logische Verknüpfungen*, wie z. B. UND, ODER und NICHT, miteinander verbunden. Die untersten Knoten sind die Ursachen, für die ihrerseits keine weiteren Ursachen bestimmt werden. Sie sind die Blätter des Baums. Der Detaillierungsgrad eines Fehlerbaums kann den Bedürfnissen der Analyse angepasst werden, indem der Baum mehr oder weniger tief verzweigt wird.
Eine FTA erfolgt gemäß [Bö6] in acht Schritten:

1. Systemanalyse durchführen
2. Unerwünschtes Ereignis (Wurzel / Top-Ereignis) und Ausfallkriterien festlegen (Wann gilt eine Komponente als ausgefallen?)
3. Relevante Zufallskenngröße und Zeitintervalle festlegen (z. B. Stunden)
4. Ausfallarten der Komponenten (Blätter) bestimmen (z. B. Kontaktunterbrechung)
5. Fehlerbaum erstellen

6. Kenngrößen der Eingänge des Fehlerbaums festlegen (z. B. Ausfallraten, Nichtverfügbarkeiten)
7. Fehlerbaum auswerten (z. B. quantitativ)
8. Ergebnisse bewerten

Eine FTA wird in der Regel als quantitative Analyse durchgeführt. Dabei werden Ausfallraten oder Gefährdungsraten des betrachteten Systems auf Basis von Bauteilausfallraten und -wahrscheinlichkeiten bestimmt. Diese Werte dienen dem Nachweis, dass das System seine geforderten Sicherheits- und Zuverlässigkeitskennwerte einhalten wird. Die FTA kann auch rein qualitativ durchgeführt werden. Dabei entfallen die Schritte 3 und 6.

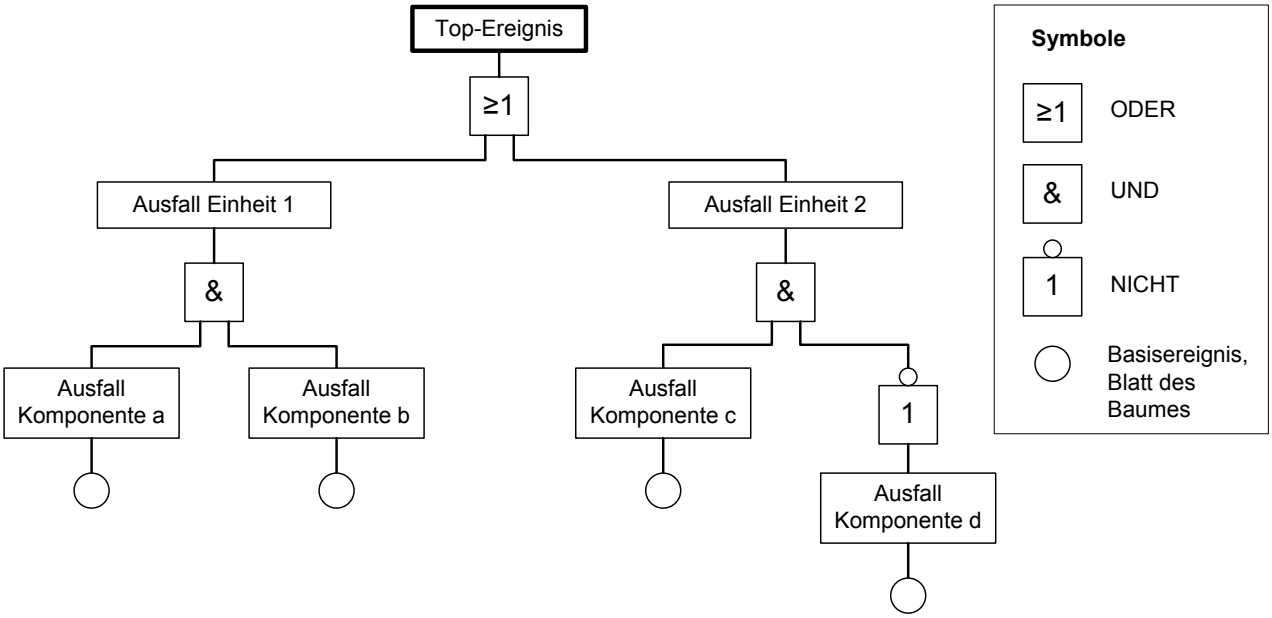

Abbildung 5.2: Qualitativer Fehlerbaum

Abbildung 5.2 zeigt ein Beispiel für einen qualitativen Fehlerbaum. Bei quantitativen Analysen werden die Knoten zusätzlich mit den entsprechenden Werten wie Ausfallwahrscheinlichkeiten, Ausfallraten oder Nichtverfügbarkeiten beschriftet. Jeder Fehlerbaum lässt sich auch als logische Gleichung schreiben. Die logische Gleichung für den in Abbildung 5.2 dargestellten Fehlerbaum lautet:
Top-Ereignis = $(A \wedge B) \vee (C \wedge \neg D)$, mit A = „Ausfall Komponente a“, für andere Ereignisse entsprechend. Diese Schreibweise dient als Grundlage für die Berechnungen der Eintretenswahrscheinlichkeit des Top-Ereignisses. Die Fehlerbaumanalyse ist genormt, siehe DIN 25424-1 [DIN81], DIN 25424-2 [DIN90a] und DIN EN 61025 [DIN07].

5.6.1 Vor- und Nachteile der Fehlerbaumanalyse

Die Fehlerbaumanalyse ist gut bekannt, gebräuchlich und weithin akzeptiert [Bra02]. Im Eisenbahnbereich ist sie eine *Standard-Methode*, die im Rahmen der Risikoanalyse und der Erstellung von Sicherheitsnachweisen verwendet wird. In der DIN EN 50129 [DIN03] ist sie als Maßnahme zur Risikoreduktion aufgeführt und für Systeme mit hohen Sicherheitsanforderungen sogar dringend empfohlen[3]. Die FTA ist gut geeignet für Systeme, deren Komponenten dauerhaft ausfallen, deren Ausfallraten konstant sind und nicht vom aktuellen Systemzustand oder einer zeitlichen Abfolge (z. B. von Ausfällen) abhängen. Die Modellierung eines Systems in Form eines Fehlerbaums erfordert neben der Fähigkeit zu strengem logischen Denken und einem soliden Systemverständnis auch

[3] Falls eine dringend empfohlene „Maßnahme nicht verwendet wird, muss die Begründung für die Nichtanwendung gegeben werden“ [DIN03].

Erfahrung im Umgang mit der Methode. Sind diese Voraussetzungen vorhanden, können mit einer FTA auch sehr komplexe Systeme hinsichtlich der Auswirkungen von Ausfallkombinationen analysiert werden.
Die FTA ist vor allem für rein *technische Systeme* geeignet. Oft besteht der Bedarf, auch den Einfluss *menschlicher Fehler* mit zu analysieren (siehe auch [SHF09]). Qualitativ ist das mit einer FTA gut möglich. Quantitativ ist die Anwendung der FTA in diesem Fall schwieriger, da menschliche Fehler nicht den gleichen Wahrscheinlichkeitsverteilungen unterliegen wie technische, insbesondere elektronische Komponenten. Ausfälle elektronischer Komponenten werden normalerweise in Form von (konstanten) Ausfallraten (Einheit: pro Stunde) angegeben, während für menschliche Fehler Wahrscheinlichkeiten (Einheit: pro Handlung) angegeben werden. Prinzipiell können in einer FTA jedoch alle Arten von Systemelementen dargestellt werden.
In einem Fehlerbaum sind stets auch die Sicherheitsmaßnahmen eines Systems enthalten, allerdings sind sie nicht explizit als solche gekennzeichnet. Eine FTA kann daher nur als Basis für eine Identifikation von Sicherheitsmaßnahmen dienen.

5.7 Ereignisbaumanalyse

Die *Ereignisbaumanalyse (ETA)* [DIN11d] ist eine weit verbreitete induktive Methode für Zuverlässigkeits-, Risiko- und Sicherheitsanalysen. Ziel einer ETA ist es zu ermitteln, was geschieht, falls ein bestimmtes *Start-Ereignis* eintritt. Die verschiedenen möglichen Folgen des Ereignisses werden in Form eines Ereignisbaums (Abbildung 5.3) von links nach rechts dargestellt. Dabei wird die zeitliche Reihenfolge des Eintretens der Ereignisse berücksichtigt.

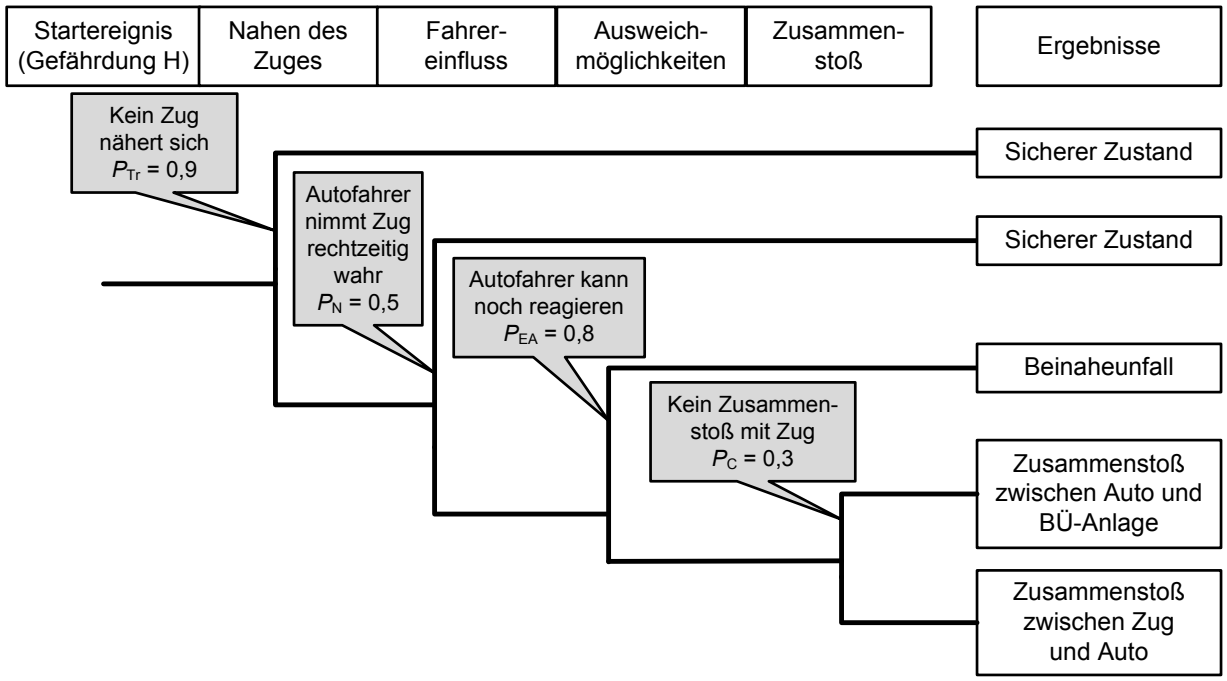

Abbildung 5.3: Ereignisbaum für eine Bahnübergangsanlage aus [DIN08]

Ausgehend vom Start-Ereignis, das die Wurzel des Baums bildet, verzweigt sich der Ereignisbaum an *schadensmindernden Faktoren* und *physikalischen Phänomenen*, die die Knoten des Baumes bilden. Schadensmindernde Faktoren sind Systeme oder Funktionen, die die Folgen des Start-Ereignisses mindern. Je nach Domäne, in der die ETA durchgeführt wird, entsprechen sie unter anderem den Begriffen Risikoreduktionsfaktor, Sicherheitsbarriere, Schutzebene oder Defence-in-Depth (siehe Abschnitt 2.3). Physikalische Phänomene sind Ereignisse oder Bedingungen, die den Verlauf der Ereignisse beeinflussen, z. B. die Entzündung einer brennbaren Flüssigkeit. Klassisch werden je Knoten

zwei Fälle unterschieden: Erfolg und Ausfall der schadensmindernden Faktoren bzw. Eintreten und Nicht-Eintreten des physikalischen Phänomens. Es sind aber auch mehr oder weniger als zwei Verzweigungen möglich. [DIN11d].

Die Blätter des Ereignisbaums werden als *Ergebnisse* bezeichnet. Sie beschreiben die End-Folgen des Start-Ereignisses (z. B. Explosion, Zusammenstoß oder auch das Einnehmen eines sicheren Zustands) unter Berücksichtigung aller wirksamen oder unwirksamen Maßnahmen. Mit Hilfe von Ausfallraten, Häufigkeiten oder Eintretenswahrscheinlichkeiten der Ereignisse kann ein Ereignisbaum quantitativ ausgewertet werden. Dadurch erhält man entsprechende Werte für die verschiedenen Ergebnisse.

Eine vollständige ETA besteht gemäß [DIN11d] aus 6 Schritten, die iterativ durchlaufen werden:

1. Systemdefinition
2. Identifikation der Start-Ereignisse
3. Identifikation von schadensmindernden Faktoren (Sicherheitsbarrieren) und physikalischen Phänomenen
4. Definition einer Reihenfolge, von Ergebnissen und quantitative Analyse
5. Analyse der Ergebnisse
6. Entscheidungen auf der Basis der Analyseergebnisse

Schritt 3 der ETA beinhaltet die Identifikation von schadensmindernden Faktoren (Sicherheitsmaßnahmen). Die Identifikation erfolgt ausgehend vom Start-Ereignis und folgt dem Verlauf der Ereignisse. Allerdings ist in der ETA kein eigenes Verfahren zur Identifikation der Barrieren enthalten. Das bedeutet, diese Identifikation erfolgt frei im Rahmen der Konstruktion der Ereignisbäume. Der Analyst folgt gedanklich den Fragen „Was passiert, wenn . . . ?“ und „Was beeinflusst das Geschehen?“.

Für den Bereich der Eisenbahn ist die ETA zur Identifikation von Barrieren im Projekt Rail Optimisation Safety Analysis (ROSA) in großem Maßstab angewendet worden [GHS+09]. Eine explizite Methode zur Identifikation der Barrieren ist in der abschließenden Dokumentation des Projekts [DBA09] jedoch nicht beschrieben worden.

Ereignisbäume können mit *Fehlerbäumen* (Abschnitt 5.6) kombiniert werden, um Wahrscheinlichkeiten für den Erfolg oder den Ausfall von Systemen zu erhalten, die als schadensmindernde Faktoren wirken. Diese Kombination entspricht dem Integrieren mehrerer Fliegendiagramme (Abschnitt 4.7) im Ereignisbaum. Für weitere Erläuterungen zur Kombination von ETA und FTA siehe [DIN11d]. Die Ereignisbaumanalyse ist durch die DIN EN 62502 [DIN11d] genormt.

5.7.1 Vor- und Nachteile der Ereignisbaumanalyse

Die Ereignisbaumanalyse (ETA) ist eine allgemein bekannte und weithin akzeptierte Methode. Im Eisenbahnbereich zählt sie zu den *Standard-Methoden*. Sie ist in der DIN EN 50129 [DIN03] als empfohlene Maßnahme zur Risikoreduktion aufgeführt und kann im Rahmen eines Sicherheitsnachweises verwendet werden.

Die ETA ist sowohl qualitativ als auch quantitativ anwendbar. Ihre Anwendung erfordert jedoch – insbesondere bei der quantitativen Anwendung – ein „hohes Expertenwissen bezüglich der Anwendung dieses Verfahrens“ [DIN11d]. Der Ereignisbaum selbst ist hingegen auch für Nicht-Experten leicht zu verstehen.

Im Gegensatz zur Fehlerbaumanalyse (FTA) ermöglicht es die ETA, die Reihenfolge und die Wechselwirkung der verschiedenen schadensmindernden Faktoren zu modellieren, die nach dem Eintreten des Start-Ereignisses Einfluss auf die Ergebnisse nehmen. Zur Betrachtung von Ausfallkombinationen ist die ETA gemäß [Bra02] nur für einfache Systeme geeignet und als eigenständige Maßnahme nicht empfohlen.

5.8 Accident Evolution and Barrier function Methode

Die *Accident Evolution and Barrier function (AEB)-Methode* von Svenson [Sve91], auch *AEB-Analyse* genannt, ist eine Methode zur Analyse von Vorfällen und Unfällen [Sve01]. Eine der Kernaufgaben der AEB-Analyse ist es, Vorschläge für neue Barrieren zu machen, um das betroffene System zu verbessern und so eine Wiederholung des Vorfalls / Unfalls zu vermeiden. Die AEB-Methode besteht gemäß [Sve91] aus sieben Schritten und nutzt dabei als Darstellungsweise das AEB-Diagramm (Abschnitt 4.9):

1. Eine Erzählung oder ein Bericht des Vorfalls wird studiert.
2. Ein wichtiger Fehler im Vorfall wird ausgewählt und in das AEB-Diagramm eintragen.
3. Frühere Fehler, die zu dem zuerst gefundenen Fehler geführt haben, werden identifiziert und in früheren Abschnitten in das Diagramm eintragen; entsprechend für tatsächliche oder hypothetische Fehler im weiteren Verlauf der Entwicklung des Vorfalls.
4. Das AEB-Diagramm wird mit Barrierefunktionen vervollständigt, die die Entwicklung zu einem Unfall aufgehalten haben oder hätten aufhalten können.
5. Jede Barrierefunktion wird analysiert und ihre Stärken und Schwächen identifiziert.
6. Die Eigenschaften des technischen und human-factors-organisatorischen Systems, die die Stärke jeder Barrierefunktion verändern könnten, werden identifiziert.
7. Eine integrierte Analyse des Vorfalls wird erstellt, zusammen mit einer Analyse möglicher Folgen für den Fall, dass sich der Vorfall zu einem Unfall weiterentwickelt hätte, und einer integrierten Analyse von Maßnahmen zur Verbesserung der Sicherheit.

Schritt 4 beinhaltet auch die Identifikation der Barrierefunktionen, die versagt haben. Ereignisse, bei denen Barrierefunktionen versagt haben, können in vielen Fällen sowohl als Fehler als auch als Versagen einer Barrierefunktion modelliert werden. Die Entscheidung drüber bleibt dem Analysten überlassen.
In einigen Fällen kann eine AEB-Analyse laut Svenson [Sve01] durch Fehlerbäume und / oder Ereignisbäume (Abschnitte 5.6 und 5.7) ergänzt werden, um weitere mögliche Fehler nach dem eigentlichen Unfall zu analysieren.

5.8.1 Vor- und Nachteile der AEB-Methode

Bei der AEB-Methode geschieht die Identifikation von Barrierefunktionen unter Zuhilfenahme anderer Analysen wie *Probabilistic Risk Assessment (PRA)* und *Human Reliability Assessment (HRA)* [Sve91]. Das bedeutet: Die eigentliche Identifikation von Barrierefunktionen hat bereits an anderer Stelle stattgefunden, und zwar bei präventiven Sicherheitsanalysen des Systems. Diese präventiven Analysen haben jedoch selten die Aufgabe, Barrierefunktionen explizit als solche zu identifizieren. Oft konzentrieren sie sich auf die Fragen, welche Gefährdungen auftreten können und wie es dazu kommen kann. Dabei werden Barrierefunktionen zwar berücksichtigt, aber selten explizit als solche benannt.
Mit der AEB-Methode werden die Fehler, die im Verlauf des Vorfalls aufgetreten sind, in eine lineare, zeitliche Reihenfolge gebracht. Zur Analyse von Ausfallkombinationen ist die Methode daher nur bedingt geeignet.
Die AEB-Methode gibt keine Anleitung dazu, welche Ereignisse in Form von Kästchen modelliert werden. Es gibt kaum Hilfestellung bei der Erstellung des AEB-Diagramms.
Die AEB-Methode hat ihren Schwerpunkt auf der Interaktion zwischen *Mensch und Technik*. Dadurch gibt sie dem bei Sicherheitsanalysen oft vernachlässigten Faktor Mensch eine gleichberechtigte Stellung in der Analyse. Allerdings ist die Methode dadurch für rein technische Systeme ungeeignet. Aufgrund der Tatsache, dass viele Systeme im Eisenbahnbereich einen hohen technischen Anteil haben, ist damit die AEB-Methode im Eisenbahnbereich nur eingeschränkt anwendbar.
Eine AEB-Analyse erfordert die Teilnahme von mehreren Experten. Unter ihnen muss laut Sven-

son [Sve01] zwingend ein *Experte für Human Factors* sein. Gerade diese Spezialisten sind jedoch nicht in jedem Unternehmen vorhanden. Dadurch ist die AEB-Analyse nicht in jedem Unternehmen durchführbar, außer mit Unterstützung durch externe Berater.

Die AEB-Methode ist vor allem für die Analyse von Unfällen und Vorfällen geeignet. Für diese Analyse muss jedoch zunächst ein Bericht vorliegen, der als Basis verwendet wird. Die AEB-Methode kann also erst in zweiter Instanz angewendet werden. Für eine präventive Systemanalyse vor einem Vorfall oder gar für die Analyse eines neuen Systementwurfs erscheint die Methode trotz anders lautender Aussage von Svenson in [Sve91] wenig geeignet. Daher ist sie auch zur Erbringung von Sicherheitsnachweisen ungeeignet.

5.9 Schutzebenenanalyse

Die *Schutzebenenanalyse* [BÖ6], auch *Layer of Protection Analysis (LOPA)* genannt, ist eine semi-quantitative Methode, die – wie der Name bereits vermuten lässt – Schutzebenen (Abschnitt 2.3.3) analysiert. Die Schutzebenen werden daraufhin untersucht, ob sie unabhängig und angemessen sind (in Zahl und Effektivität), um ein bestimmtes Risiko auf ein akzeptables Maß zu reduzieren. LOPA ist eine Anpassung der Ereignisbaumanalyse (ETA) (Abschnitt 5.7) auf die Bedürfnisse der Prozessindustrie. Der wesentlichste Unterschied zur Ereignisbaumanalyse ist, dass nur eine eingeschränkte Menge an schadensmindernden Faktoren zugelassen wird.

Bei LOPA wird jeweils ein *Szenario* analysiert: ein Ursache-Folge-Paar, in der Regel mit Zwischenschritten. Zwischenschritte sind hierbei vor allem mehrere Schutzmaßnahmen. Um Schutzebenen analysieren zu können, müssen diese zunächst identifiziert werden – mit Bezug auf das betrachtete Szenario. Diese Identifikation ist jedoch nicht Bestandteil der Schutzebenenanalyse selbst. LOPA bedient sich zu diesem Zweck idealerweise einer *vorgelagerten qualitativen Gefährdungsanalyse*, z. B. *Hazard and Operability Studies (HAZOP)* [Sum03]. Während die vorgelagerte Analyse mögliche Schutzmaßnahmen identifiziert, bewertet LOPA diese Schutzmaßnahmen daraufhin, ob sie geeignet sind, als *unabhängige Schutzebenen (USE)* das bestehende Risiko zu reduzieren, und wie stark sie dies tun. LOPA ist ebenfalls geeignet, um Sicherheitsintegritätslevel (SIL) für Funktionen / Systeme zu bestimmen (siehe z. B. [Las08]).

Es gibt in der Literatur zahlreiche Beschreibungen von LOPA, z. B. [Cen01], [DH02], [BÖ6] und [DIN05b]. Die Beschreibungen des Vorgehens bei der Analyse sind stets leicht unterschiedlich, daher wird hier nur auf die wesentlichen Schritte einer LOPA eingegangen. LOPA besteht im Wesentlichen aus den folgenden Schritten:

- Eine unerwünschte Folge / Gefährdung auswählen
- Alle auslösenden Ursachen identifizieren und ihre Häufigkeiten abschätzen (semi-quantitativ, in Größenordnungen)
- Ein Szenario bilden: Kombination der Folge mit einer möglichen Ursache zu einem Ursache-Folge-Paar
- Für dieses Szenario: Prüfen der Schutzmaßnahmen dahingehend, ob sie für das Szenario wirksam sind und ob sie USE sind. Hierzu wird eine Liste mit Kriterien verwendet, die sogenannten „3 D's“, „4 E's“ und das „Big I“ (siehe [BÖ6]).
- Für dieses Szenario: Wahrscheinlichkeit für das Eintreten der Folge bestimmen (semi-quantitativ, in Größenordnungen), Risiko bestimmen
- Bei Bedarf geeignete Verbesserungsmaßnahmen empfehlen
- Übergang zum nächsten Szenario

LOPA verwendet implizit das Zwiebelschalenmodell (ZSM) (Abschnitt 4.3) [BÖ6]. Als Darstellung können aber auch das LOPA-Diagramm (Abschnitt 4.4) oder der Ereignisbaum verwendet werden (Abbildung 5.4). Die Dokumentation der Analyse wird durch ein Formblatt unterstützt [DH02].

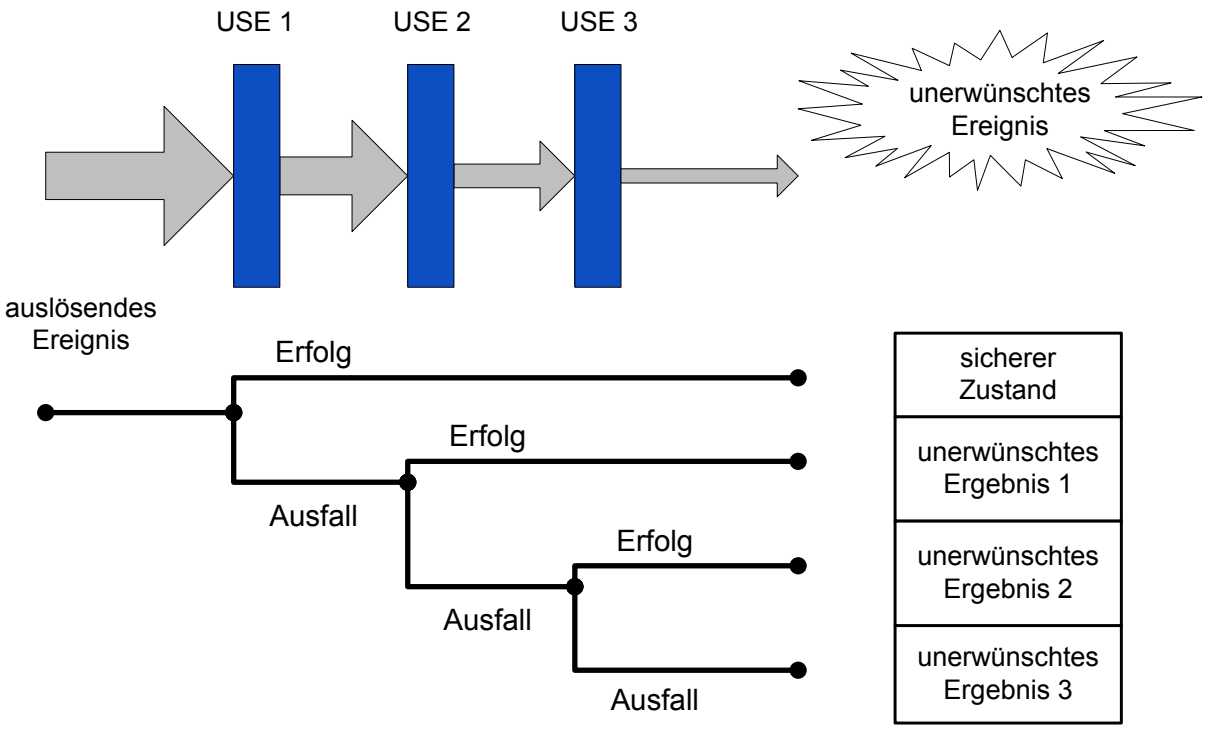

Abbildung 5.4: Gegenüberstellung eines LOPA-Diagramms mit einem Ereignisbaum in Anlehnung an Dowell et al. [DH02]

5.9.1 Vor- und Nachteile der Schutzebenenanalyse

Bei der Schutzebenenanalyse (LOPA) geschieht die Identifikation von Barrieren unter Zuhilfenahme anderer Analysen, wie z. B. HAZOP. Die eigentliche Identifikation hat bereits an anderer Stelle stattgefunden. Im Rahmen von LOPA werden die Schutzebenen nur noch *bewertet*. Es wird für jedes Szenario nur eine Störung des Prozesses als auslösende Ursache betrachtet. Zwar werden durch die Betrachtung mehrerer USE Mehrfachausfälle berücksichtigt, dies gilt aber nur für Ausfälle von USE. Kombinationen von auslösenden Ereignissen werden nicht betrachtet. Für das betrachtete Szenario wird das Risiko semi-quantitativ bestimmt. Die Schutzebenenanalyse legt *strenge Kriterien* an die USE an, was dazu führt, dass nicht alle Barrieren (oder schadensmindernde Faktoren, wie sie in der ETA genannt werden), bei der Analyse berücksichtigt werden. Dadurch ist die Risikoabschätzung konservativ, d. h. das tatsächliche Risiko ist möglicherweise geringer als das durch die Analyse ermittelte.

Anwendungen der LOPA im Eisenbahnbereich sind bisher nicht bekannt, aber durchaus vorstellbar. Allerdings ist im Eisenbahnbereich eher die Anwendung der Standard-Methode ETA anstatt der von ihr abgeleiteten LOPA zu empfehlen. Daher sind die Ergebnisse der LOPA für Sicherheitsnachweise nur eingeschränkt verwendbar.

5.10 Vergleich der Methoden

Tabelle 5.3 zeigt einen Vergleich der untersuchten Methoden aus den Abschnitten 5.3 bis 5.9. Dabei wird bewertet, inwiefern die einzelnen Methoden die Anforderungen M-1 bis M-12 erfüllen. Um den Vergleich zwischen den Methoden zu vervollständigen, werden in Tabelle 5.3 zusätzlich noch folgende Punkte bewertet:

Sicherheitsmaßnahmen-Bewertung: Werden die Sicherheitsmaßnahmen durch die Methode bewertet? Wenn ja, wie groß ist die methodische Hilfestellung dabei?

Unfall: Ist die Methode geeignet, um tatsächlich geschehene Unfälle sowie den Unfallhergang zu analysieren?

Für die Bewertung werden die folgenden Kategorien verwendet:

\+ ja / sehr
o eingeschränkt / möglich / mittel
\- nein / wenig / nicht dazu gedacht

Tabelle 5.3: Vergleich vorhandener Methoden sowie Auswahl der für den Zweck der vorliegenden Arbeit am besten geeigneten Methoden, wie im Text erläutert

Methode	Darstellungsweise (M-8)	Sicherheitsmaßn.-Id. (M-1)	Sicherheitsmaßn.-Bewertung	quantitativ (M-2)	Eisenbahn (M-3)	generisch (M-4)	SiNa-tauglich (M-5)	Systemelemente (M-6)	leicht zu erlernen (M-7)	Standard (Bahn) (M-7)	präventiv (M-9)	Unfall	Ausfallkombinationen (M-10)	deduktiv (M-11)	induktiv (M-12)
WBA	WBG	o	-	-	+	-	-	+	o	-	-	+	+	+	-
SFA	Text	o	+	o	+	+	o	+	o	-	+	+	-	o	-
BA	Energiemodell	+	+	-	+	+	o	+	+	-	+	o	o	-	+
FTA	Fehlerbaum	o	o	+	+	+	+	+	o	+	+	-	+	+	-
ETA	Ereignisbaum	o	+	+	+	+	+	+	o	+	+	-	o	-	+
AEB	AEB-Diagramm	o	+	-	o	-	-	o	o	-	-	+	o	o	o
LOPA	LOPA-Diagramm, ZSM, Ereignisbaum	-	+	o	o	+	o	+	o	-	+	-	o	-	+

Die Auswahl der am besten geeigneten Methoden erfolgt unter Zuhilfenahme der Bewertung aus Tabelle 5.3. Zusätzlich wird berücksichtigt, wie wichtig die Erfüllung der einzelnen Anforderungen M-1 bis M-12 sowie der weiteren Kriterien im Hinblick auf das Ziel der vorliegenden Arbeit ist.
Von den untersuchten Methoden erfüllt keine alle Anforderungen an die gesuchte Methode. Jedoch besitzen die Barriereanalyse (BA), die Fehlerbaumanalyse (FTA) und die Ereignisbaumanalyse (ETA) viele positive Eigenschaften, was sich auch in den vielen positiven Bewertungen (+) in Tabelle 5.3 ausdrückt. Diese drei Methoden erfüllen die meisten der Anforderungen M-1 bis M-12.
In der DIN EN 50129 [DIN03] wird gefordert, deduktive und induktive Methoden zu kombinieren (Anforderungen M-11 und M-12). Daher soll im Folgenden die **FTA** als deduktive Methode zusammen mit einer induktiven Methode (BA oder ETA) als Basis für eine Identifikation von Sicherheitsschichten verwendet werden. Die **BA** bietet als einzige der untersuchten Methoden eine starke methodische Unterstützung bei der Identifikation von Sicherheitsmaßnahmen durch den Einsatz von *Checklisten*. Zudem ist sie von allen untersuchten Methoden am leichtesten zu erlernen. Aufgrund dieser Vorteile ist sie für den Zweck der vorliegenden Arbeit besser geeignet als die ETA. Aufgrund dieser

Argumentation wird im Folgenden der Ansatz verfolgt, diese beiden Methoden **BA und FTA** zur Identifikation von Sicherheitsschichten zu kombinieren. Um so eine Methode zu erhalten, die für den Zweck der vorliegenden Arbeit vollständig geeignet ist, müssen jedoch folgende Lücken geschlossen werden:

- Eine Anleitung, wie mit Hilfe der FTA Sicherheitsmaßnahmen bzw. Sicherheitsschichten identifiziert werden können, fehlt.
- Eine Anleitung, wie mit Hilfe der BA nicht nur Barrieren, sondern Sicherheitsschichten identifiziert werden können, fehlt.
- Die vorhandenen Checklisten der BA sind noch zu grob und nicht auf den Eisenbahnbereich angepasst.

Im nachfolgenden Kapitel werden Wege aufgezeigt, um diese Lücken zu schließen. Es wird eine *neue Methode* entwickelt, die die Vorteile von BA und FTA kombiniert und dadurch die Sicherheitsschichten eines Systems identifizieren kann.

6 ISES-Methode

Im Folgenden wird eine neue Methode zur Identifikation der Sicherheitsschichten eines Eisenbahnsystems vorgestellt. Die einzelnen Schritte der Methode werden anhand eines kleinen Beispiels verdeutlicht. In Kapitel 8 wird diese Methode auf das umfangreichere Beispiel eines Bahnübergangs angewendet, um das Verständnis der Anwendung der Methode zu vertiefen.

6.1 Gesamtrahmen der Methode zur Identifikation von Sicherheitsschichten

Zweck der gesuchten Methode ist es, Sicherheitsschichten in Eisenbahnsystemen zu identifizieren. Dabei soll sie die in Abschnitt 5.1 genannten Anforderungen M-1 bis M-12 erfüllen. Aufgrund ihres Zwecks wird die neue Methode als **ISES-Methode** (Methode zur Identifikation von Sicherheitsschichten in Eisenbahnsystemen) bezeichnet.
Wie in Abschnitt 5.10 festgestellt, erfüllt keine der Methoden aus Kapitel 5 alle Anforderungen. Daher sollen im Folgenden die in Abschnitt 5.10 ausgewählten Methoden, Fehlerbaumanalyse (FTA) und Barriereanalyse (BA), zur neuen ISES-Methode zusammengefügt und dabei die in Abschnitt 5.10 genannten Lücken geschlossen werden. Eine Kombination der ausgewählten Methoden ermöglicht es, ihre jeweiligen Vorteile zu nutzen und dabei die methodischen Anforderungen der DIN EN 50129 [DIN03] zu berücksichtigen.
Daher wird folgender Ansatz, bestehend aus vier Schritten, verwendet (siehe auch Abbildung 6.1):

A: Fehlerbaumanalyse (FTA) für das betrachtete System
B: Identifikation von unabhängigen Sicherheitsbarrieren mit Hilfe des Fehlerbaums aus der FTA
C: Bestimmung weiterer Sicherheitsbarrieren und ihrer Funktionen mit Hilfe von Checklisten
D: Prüfen der Sicherheitsbarrieren und Funktionen auf die Kriterien für Sicherheitsschichten (Wirksamkeit und Unabhängigkeit) und Bestimmung der Sicherheitsschichten

Neben den Schritten A bis D gehören zur ISES-Methode, wie zu jeder Methode, selbstverständlich noch *Vor- und Nachbereitung*. Bei der Vorbereitung werden z. B. Ziele definiert, das Team zusammengestellt, Eingangsdaten zusammengetragen, die Art der Dokumentation festgelegt und ein Zeitplan aufgestellt. Bei der Nachbereitung geht es vor allem um die Erstellung eines Berichts mit einer Zusammenfassung der Ergebnisse, der Ableitung von Handlungsvorschlägen und ggf. der Planung weiterer Maßnahmen wie z. B. der Pflege der Analyse und ihre Anpassung an den Fortschritt des Projekts zu gegebener Zeit. Diese Vor- und Nachbereitung sind allgemein Bestandteil jeder Analyse und somit jeder Methode. Da sie keine Besonderheit der ISES-Methode darstellen, wird auf die Vor- und Nachbereitung an dieser Stelle nicht weiter eingegangen.
Im folgenden Abschnitt werden zunächst die Voraussetzungen zur Anwendung der ISES-Methode erörtert. Anschließend werden die Schritte A bis D der Methode ausführlich erläutert. Zu jedem Schritt werden die Ziele, die derzeitige Situation, in die sich der Schritt einfügt, die Voraussetzungen, die eigentliche Durchführung und die Ergebnisse beschrieben. Unterstützt wird die Erläuterung der einzelnen Schritte durch ein durchgehendes Beispiel. Abschließend findet eine Bewertung jedes einzelnen Schritts statt.

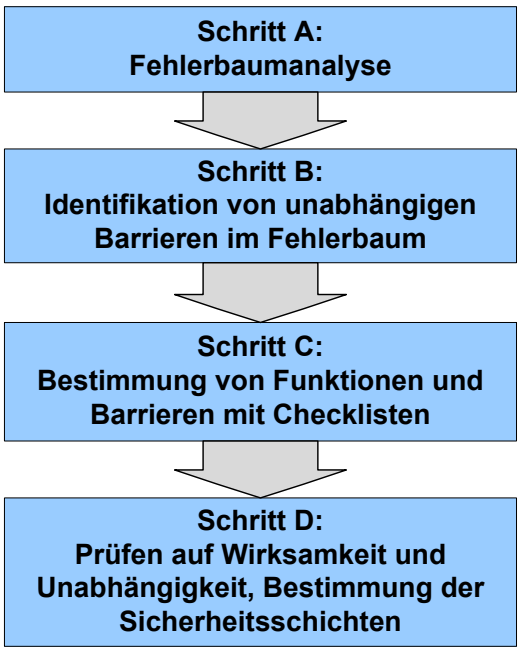

Abbildung 6.1: ISES-Methode (Methode zur Identifikation von Sicherheitsschichten in Eisenbahnsystemen)

6.2 Voraussetzungen für die Anwendung der ISES-Methode

Eine Methode ist nicht für alle Probleme / Systeme gleichermaßen gut anwendbar. Hier soll erläutert werden, für welche Systeme die ISES-Methode gut und für welche sie weniger gut geeignet ist.

Der erste Schritt der Methode ist eine Fehlerbaumanalyse (FTA). Da die FTA ein Bestandteil der Methode ist, ist die ISES-Methode nur für solche Systeme geeignet, die sich für eine Analyse mittels FTA eignen.

Laut einer vergleichenden Analyse von Methoden von Braband [Bra02] ist eine FTA für komplexe Systeme und auch für neue Systementwürfe geeignet. Die FTA ist jedoch nicht geeignet, um zu analysieren, inwiefern das Systemverhalten von der Reihenfolge der unerwünschten Ereignisse bzw. der Ausfälle abhängt. Wird sie dennoch angewendet, muss die Information über die Reihenfolgeabhängigkeit verworfen werden. Stattdessen wird das System vereinfacht modelliert. Für die meisten in der Praxis verwendeten Systeme ist die FTA jedoch eine geeignete Analysemethode.

Entsprechend der Einschränkungen bei der FTA kann bei Systemen, deren Verhalten sehr stark von der Reihenfolge der Ereignisse bzw. Ausfälle abhängt, die ISES-Methode zwar angewandt werden, allerdings geht hierbei die Information über die Reihenfolgeabhängigkeit verloren. Der Analyst muss hier entscheiden, ob die Modellierung in Form von Sicherheitsschichten das Sicherheitsverhalten seines Systems noch ausreichend korrekt wiedergibt, wie wichtig die Reihenfolgeabhängigkeit ist und ob ggf. eine andere Methode verwendet werden sollte.

Insgesamt ist die ISES-Methode sowohl für Systeme geeignet, die rein technische Systeme sind, als auch für solche, bei denen Mensch und Technik zusammenwirken. Sie ist für einfache und komplexe Systeme geeignet. Sie kann sowohl zur Analyse bestehender Systeme als auch für neue Entwürfe eingesetzt werden.

6.3 Schritt A: Fehlerbaumanalyse für das System

Das *Ziel* des Schritts A ist es, für die zu betrachtende Gefährdung des zu untersuchenden Systems einen qualitativen Fehlerbaum zu erhalten. Dieser Fehlerbaum wird im nachfolgenden Schritt B weiter analysiert.

6.3.1 Situation

Die FTA (Abschnitt 5.6) ist eine weit verbreitete und weithin akzeptierte Methode zur Analyse von Systemausfällen. Es ist bei Bahnsystemen üblich, vor Inbetriebnahme des Systems eine solche Analyse durchzuführen. Die DIN EN 50129 [DIN03] empfiehlt die Anwendung der FTA zur Analyse von Mehrfachausfällen, insbesondere für Systeme mit hohen Sicherheitsanforderungen. Häufig kommt die FTA im Rahmen der Sicherheitsnachweisführung zum Einsatz. Sie ist dann meist sogar quantitativ und dient dem Nachweis, dass das System die vorgegebene tolerierbare Gefährdungsrate (THR) nicht überschreitet. Aber auch qualitativ werden Fehlerbäume verwendet, z. B. im Rahmen des Sicherheitsnachweises gemäß der Sicherheitsrichtlinie Fahrzeug (SIRF) [EBVVD12].

Da eine FTA in vielen Fällen ohnehin mit Bezug auf die Sicherheit durchgeführt wird, macht es Sinn, sie noch weiter zu nutzen. Hinzu kommt, dass schon Harms-Ringdahl [HR09], Hollnagel [Hol99] und Sklet [Skl04] auf den Zusammenhang zwischen Fehlerbäumen und Barrieren hinweisen. Die FTA ist daher ein guter Ansatz zur Identifikation von Barrieren.

6.3.2 Voraussetzungen

Bevor mit dem eigentlichen Schritt A begonnen werden kann, müssen zunächst das zu analysierende *System* und seine *Grenzen* festgelegt werden. Des Weiteren müssen die relevanten, zu betrachtenden *Gefährdungen* bereits identifiziert worden sein. Dazu kann z. B. auf bereits existierende Kataloge von Gefährdungen (siehe z. B. Projekt *Rail Optimisation Safety Analysis (ROSA)* [GHGP09a]) zurückgegriffen werden. Von diesen Gefährdungen muss *eine* für die nachfolgende Analyse ausgewählt werden.

Liegt noch keine FTA für die zu betrachtende Gefährdung vor, muss zunächst geklärt werden, ob das System zur Analyse durch eine FTA *geeignet* ist. Es müssen die notwendigen Eingangsdokumente für eine qualitative FTA wie z. B. eine geeignete Systembeschreibung beschafft werden. Diese Dokumente müssen ausreichend Informationen darüber enthalten, wie stark das Systemverhalten von der Reihenfolge der Ereignisse abhängt, damit entschieden werden kann, ob sich das Ausfallverhalten des Systems in Form eines Fehlerbaums darstellen lässt. In den meisten Fällen wird diese Entscheidung positiv ausfallen – es kann eine FTA durchgeführt werden.

Liegt bereits eine FTA vor, dann muss geprüft werden, ob sie in einer für die jetzt folgende Analyse geeigneten Form und Detaillierungstiefe vorliegt. Ist das nicht der Fall, muss die FTA in Schritt A überarbeitet und angepasst werden.

Für den Zweck der ISES-Methode ist es nicht notwendig, quantitative Daten wie Wahrscheinlichkeiten und Ausfallraten für die Ereignisse bzw. Komponenten des Systems zu beschaffen. Die FTA wird *rein qualitativ* durchgeführt. Im Hinblick auf möglich spätere, weiterführende quantitative Untersuchungen kann eine entsprechende Datenbasis jedoch von Nutzen sein.

Neben der Prüfung, ob das System für die Anwendung der Methode geeignet ist, müssen auch die *organisatorischen Rahmenbedingungen* für die Durchführung einer Analyse mit der ISES-Methode geprüft werden: Sind ausreichend Zeit und Budget vorhanden? Steht fachlich qualifiziertes Personal bzgl. der Methode als auch bzgl. des Systems zur Verfügung?

6.3.3 Durchführung

Liegt noch keine FTA für die zu betrachtende Gefährdung vor, so wird für diese Gefährdung eine qualitative FTA gemäß den üblichen Beschreibungen der Methode (z. B. [DIN81], [VGRH81], [Eri05] oder [BÖ06]) durchgeführt. Der quantitative Teil der FTA entfällt.
Wichtig bei der Fehlerbaumanalyse als Hilfsmittel zur Identifikation von Sicherheitsschichten (SiS) ist, dass der Fehlerbaum für eine festgelegte Top-Level-Gefährdung erstellt wird. Er muss das gesamte (zuvor festgelegte) System umfassen und bis zu einer geeigneten Ebene detailliert werden. Diese Ebene ist eine Subsystemebene, sie ist nicht rein funktional, sondern umfasst „große Hardware-Komponenten“, z. B. ein ganzes Signal oder ein Signalgeber eines Signals. Die Ebene „ein Stellwerk“ wäre zu grob, „ein Relais“ zu detailliert. Dazwischen bleibt dem Analysten Spielraum, den Detaillierungsgrad seinen Bedürfnissen anzupassen.
Mit Hinblick auf die weiteren Schritte der ISES-Methode sollte der Fehlerbaum in den verschiedenen Zweigen idealerweise so weit entwickelt werden, wie ausschließlich UND-Verknüpfungen im Baum auftreten. Treten erste ODER-Verknüpfungen auf, *kann* für die Suche nach Sicherheitsschichten ein Abbruchkriterium vorliegen, sodass eine Weiterentwicklung des Fehlerbaums mitunter nicht notwendig ist. Allerdings ist nicht jede ODER-Verknüpfung zwangsläufig ein Abbruchkriterium (siehe Abschnitt 6.4). Um den Fehlerbaum möglichst minimal zu gestalten und dadurch Aufwand zu sparen, kann der Analyst den Fehlerbaum zunächst bis zu den ersten auftretenden ODER-Verknüpfungen entwickeln. Nach der Durchführung von Schritt B sollte der Fehlerbaum dann ggf. an einzelnen Stellen noch weiter entwickelt werden. Dieses Vorgehen empfiehlt sich jedoch nur, wenn der Ersteller des Fehlerbaums und der Anwender der ISES-Methode eng zusammenarbeiten.
Wird der Fehlerbaum nicht ausschließlich für die Identifikation von Sicherheitsschichten erstellt, so wird die Detaillierungstiefe meist durch die vorliegenden Informationen (Systembeschreibung, Anteil Eigenentwicklung / Zukaufteile, vorhandene Ausfallraten etc.) bestimmt. Ein Fehlerbaum, der für eine Berechnung einer Gefährdungsrate erstellt wird, ist in der Regel detailliert genug, um zur Durchführung der ISES-Methode genutzt zu werden.
Für die nachfolgenden Schritte ist es notwendig, dass im Fehlerbaum keine Ereignisdopplungen auftreten. Das bedeutet, jedes Ereignis (jeder Ausfall einer Komponente) darf im Fehlerbaum nicht mehr als einmal auftreten. Der Fehlerbaum ist dann nicht vermascht, er ist ein echter Baum, also kreislos.

6.3.4 Ergebnis

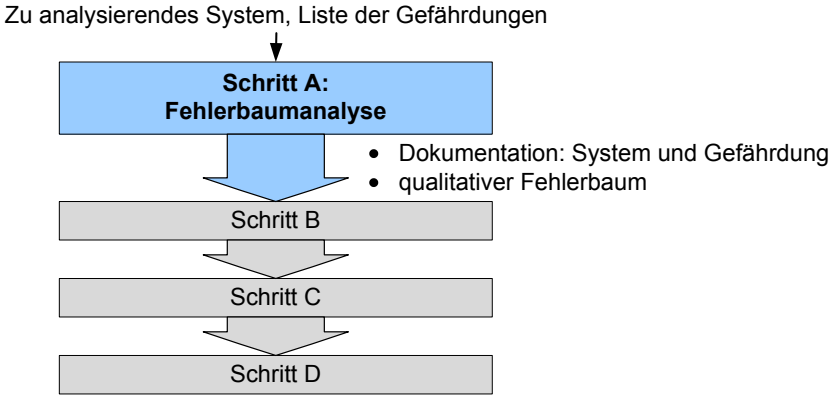

Abbildung 6.2: Schritt A der ISES-Methode

Ein Ergebnis dieses Schritts besteht in der Beschreibung des analysierten Systems inklusive seiner Systemgrenzen. In der Dokumentation der Analyse wird ebenfalls die betrachtete Gefährdung ver-

merkt. Ein weiteres Ergebnis besteht in dem erstellten bzw. überarbeiteten qualitativen Fehlerbaum für die betrachtete Gefährdung. Dieser Fehlerbaum enthält keine Ereignisdopplungen.

6.3.5 Beispiel

Als Beispiel zur Verdeutlichung der Methode soll ein kleines, vereinfachtes Beispiel aus dem Bereich der Eisenbahn dienen. Dieses Beispiel-System hat eine wichtige, sicherheitsrelevante Aufgabe: die Geschwindigkeitsüberwachung und -reduktion eines Zuges. Das Beispiel entstammt zwar der Praxis, wurde zur Demonstration der Methode jedoch abgewandelt und stark vereinfacht.
An diesem Beispiel werden alle Schritte der ISES-Methode demonstriert und erläutert, wobei der Schwerpunkt auf der prinzipiellen Erläuterung der Methode und nicht auf der Vollständigkeit liegt. Daher werden alle Ergebnisse nur kurz umrissen. Ein ausführlicheres Beispiel zur Anwendung der ISES-Methode wird in Kapitel 9 vorgestellt.
Das zu analysierende System soll als Aufgabe die Geschwindigkeitsüberwachung und -reduktion eines Zuges in einer bestimmten, zeitlich oder räumlich befristeten Situation haben, z. B. bei einer temporären Langsamfahrstelle. Es umfasst den Triebfahrzeugführer (Tf), den Tachometer und ein technisches Überwachungssystem, das den Zug bei zu hoher Geschwindigkeit bremsen kann. Dafür stehen zwei unabhängige Bremssysteme zur Verfügung. Das technische Überwachungssystem soll nicht permanent aktiv sein, sondern wird durch bestimmte Trigger, auf die hier nicht näher eingegangen werden soll, an- und ausgeschaltet. Sämtliche Bestandteile dieses fiktiven Systems sind in Abbildung 6.3 dargestellt. Diese „Systembeschreibung“ ist in der Praxis etwas zu kurz, soll aber für das Beispiel an dieser Stelle genügen.

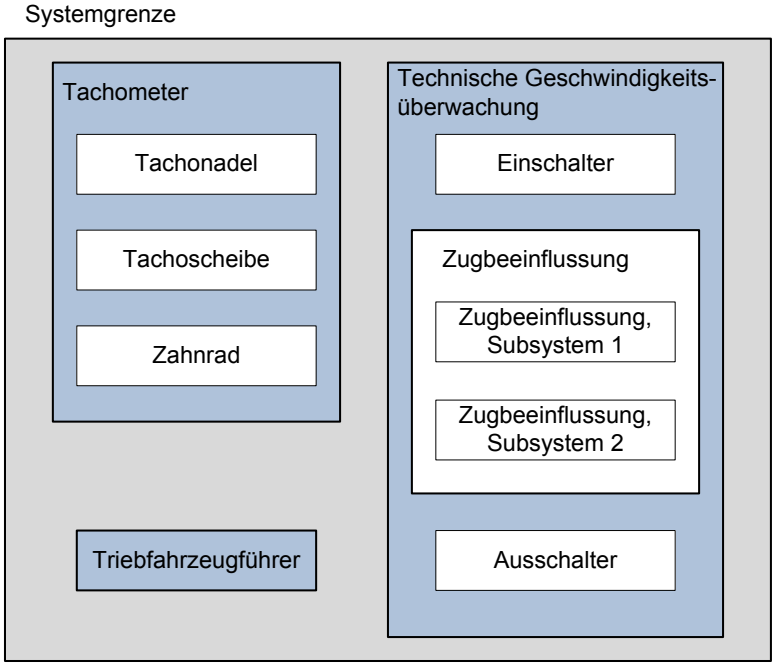

Abbildung 6.3: Beispiel-System zur Geschwindigkeitsüberwachung

Als nächstes muss die zu betrachtende Gefährdung festgelegt werden. Für das Beispiel soll die folgende Gefährdung untersucht werden: *überhöhte Geschwindigkeit*.
Für diese Gefährdung wird anschließend eine qualitative FTA durchgeführt, deren Fehlerbaum in Abbildung 6.4 dargestellt ist. Dieser Fehlerbaum ist für das Beispiel stark vereinfacht worden. Insbesondere wurde nicht berücksichtigt, dass auch der Tf in einem realen System die Möglichkeit hat, den Zug zu bremsen. Der Fehlerbaum enthält jedoch alle zur Demonstration der ISES-Methode notwendigen Elemente.

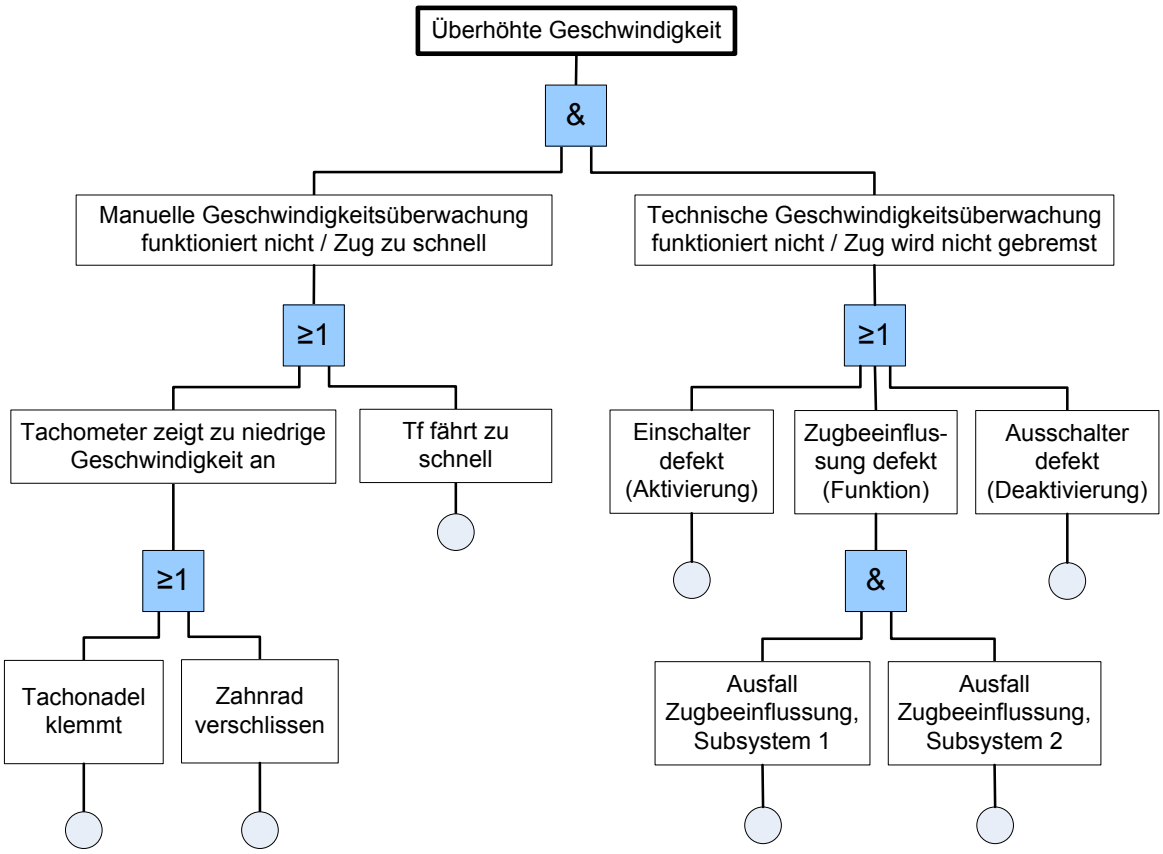

Abbildung 6.4: Fehlerbaum für das Beispiel-System zur Geschwindigkeitsüberwachung

6.3.6 Bewertung

Kernpunkt einer FTA ist die Betrachtung von Kombinationen von Ausfällen in einem System. Dadurch ist sie gut geeignet als Grundlage für eine Analyse der Sicherheitsschichten eines Systems. Eine FTA ermöglicht eine quantitative Analyse, sodass durch die Wahl der FTA eine gute Voraussetzung für eine spätere quantitative Bewertung der Sicherheitsschichten geschaffen wird.

Für die Durchführung einer FTA ist Fachwissen erforderlich. Dies betrifft sowohl die Methode FTA als auch das zu analysierende System. Daher ist die Anwendung im Team zu empfehlen. Alle an der Analyse beteiligten Personen müssen in der Anwendung der FTA geschult sein. Mindestens ein Teammitglied sollte bereits Erfahrungen mit FTA gesammelt haben.

Der Schwierigkeitsgrad dieses Schritts entspricht dem Schwierigkeitsgrad einer FTA: Je nach Komplexität des betrachteten Systems liegt dieser zwischen durchschnittlich schwierig bis anspruchsvoll. Da die Methode FTA im Eisenbahnbereich sehr gebräuchlich ist, stellt dieser Schwierigkeitsgrad jedoch kein Hindernis für die Anwendung der ISES-Methode dar.

Da hier mit der FTA eine Methode genutzt wird, die im Rahmen der Sicherheitsnachweisführung allgemein akzeptiert ist und oft eingesetzt wird, ist der effektive Zeitbedarf relativ gering, da in vielen Fällen die FTA ohnehin durchgeführt wird. Am Markt sind zahlreiche Software-Tools verfügbar, die die Analysten bei der Erstellung des Fehlerbaums unterstützen. Durch die bildliche, logische Darstellung des Ergebnisses als Fehlerbaums, ist die Interpretation des Ergebnisses wesentlich einfacher als seine Erstellung.

6.4 Schritt B: Identifikation von Barrieren mit Hilfe der Fehlerbaumanalyse

Das *Ziel* des Schritts B ist es, mit Hilfe des Fehlerbaums aus Schritt A die im System vorhandenen unabhängigen Barrieren zu identifizieren.

6.4.1 Situation

Eine Sicherheitsschicht besteht aus einer Barriere und ihrer Funktion (siehe Kapitel 3). Den meisten Menschen fällt es leichter, in technischen Systemen als in Funktionen zu denken. Sie denken bevorzugt in technisch realisierten Prozessen wie „dann löst das Sicherheitsventil aus und es kann nichts mehr passieren“ statt in abstrakten Funktionen wie „Überdruck erkennen“ und „Überdruck ablassen“. Deshalb fällt es vielen Menschen schwer, sich den funktionalen Ansatz der Sicherheitsnormen (DIN EN 50126-1 [DIN00], DIN EN 61508 [DIN11a] – [DIN11c]) zu eigen zu machen. Zur Identifikation von Sicherheitsschichten ist es daher sinnvoll, zunächst auf die technische Ebene zu gehen und die verwendeten Barrieren zu betrachten.
(Sicherheits-)Barrieren reduzieren das Unfallrisiko. Daher hat ihre Kenntnis direkten Einfluss auf die Sicherheitsanforderungen an das System und die verwendeten Komponenten.
In der Literatur finden sich bei mehreren Autoren Hinweise darauf, dass in Fehlerbäumen Barrieren enthalten sind, z. B. bei Harms-Ringdahl: „In fault trees and event trees, the barriers are clearly modelled“ [HR09]. Auch Hollnagel gibt an, dass Barrieren in Fehlerbäumen einfach zu finden seien: „Once the fault tree has been constructed possible barriers can be explored simply by considering each of the branches of the tree“ [Hol99]. Auch Rådbo [RSA08] nutzt Fehlerbäume, um potenzielle Barrieren zu identifizieren. Alle diese Autoren geben jedoch keine konkrete Anleitung, wo oder wie in einem Fehlerbaum Barrieren zu finden sind. Johnsen et al. schreiben in [JHVR06], dass sicherheitskritische Funktionen den Basisereignissen in einer FTA oder den Barrieren in einer Ereignisbaumanalyse (ETA) entsprechen. Wenn die sicherheitskritischen Funktionen in etwa den Barrieren bzw. ihren Funktionen entsprechen, dann müssten die Barrieren in den Basisereignissen eines Fehlerbaums, also in seinen Blättern zu finden sein.
Dieser Ansatz soll anhand eines Beispiel-Fehlerbaums näher untersucht werden, der in Abbildung 6.5 dargestellt ist. Dieser Fehlerbaum ist ein Ausschnitt[1] aus einem Fehlerbaum für einen Bahnübergang mit Überwachungssignal und punktförmiger Zugbeeinflussung (PZB), der bereits in [Sch10] präsentiert wurde. Der Fehlerbaum aus Abbildung 6.5 besitzt sieben Blätter:

- Tf reagiert zu spät
- Tf erkennt Gefahr nicht
- Übertragung Magnet – fahrzeugseitige PZB fehlerhaft
- Defekt 1000-Hz-Magnet
- PZB wirkt fahrzeugseitig nicht
- ÜS zeigt nicht Halt
- Tf übersieht Halt zeigendes ÜS

Nach der eben beschriebenen Vorgehensweise machen diese sieben Blätter Hoffnung auf sieben Barrieren bzw. Barrierefunktionen. Doch welche sind das? Das Reagieren des Tf? Das Erkennen der Gefahr? Die Übertragung zwischen PZB-Magnet und fahrzeugseitiger PZB? Der 1000-Hz-Magnet? Die fahrzeugseitige PZB? Das Halt Zeigen des Signals? Das Sehen des Signals durch den Tf?
Beim Betrachten dieser Liste fällt Folgendes auf:

- Der Tf kommt mehrfach vor, er hat mehrere Funktionen. Diese Funktionen sind daher nicht unabhängig voneinander implementiert.

[1] Der vollständige Fehlerbaum ist im Anhang A wiedergegeben.

- Der-1000-Hz Magnet der PZB ist eigentlich keine Barriere, denn er allein kann nichts bewirken. Erst zusammen mit der Übertragung und der fahrzeugseitigen PZB lässt sich eine Wirkung erzielen. Fällt der Magnet hingegen aus, dann kann auch die fahrzeugseitige PZB nicht mehr eingreifen.
- Das Halt zeigende Signal ist eine Barriere, wie man sie sich typischerweise vorstellt.
- Die Ebene, bis zu der die FTA durchgeführt wird, ist abhängig vom Zweck der Analyse und von den zur Verfügung stehenden Daten. Werden die Blätter des Fehlerbaums als Barrieren betrachtet, so ergeben sich dadurch Barrieren auf höchst unterschiedlichen Detailstufen.
- Wird der Fehlerbaum noch weiter detailliert, wird irgendwann die Bauteilebene erreicht: Kondensatoren, Leitungen, Leuchtmittel, Relais etc. Diese Bauteile werden dann zum Ansatzpunkt für die Suche nach Barrieren: Barriere 1: Relais A, Barriere 2: Relais B, Barriere 3: Leuchtmittel A etc. Diese Ebene ist viel zu detailliert, um Barrieren für Sicherheitsschichten zu identifizieren.

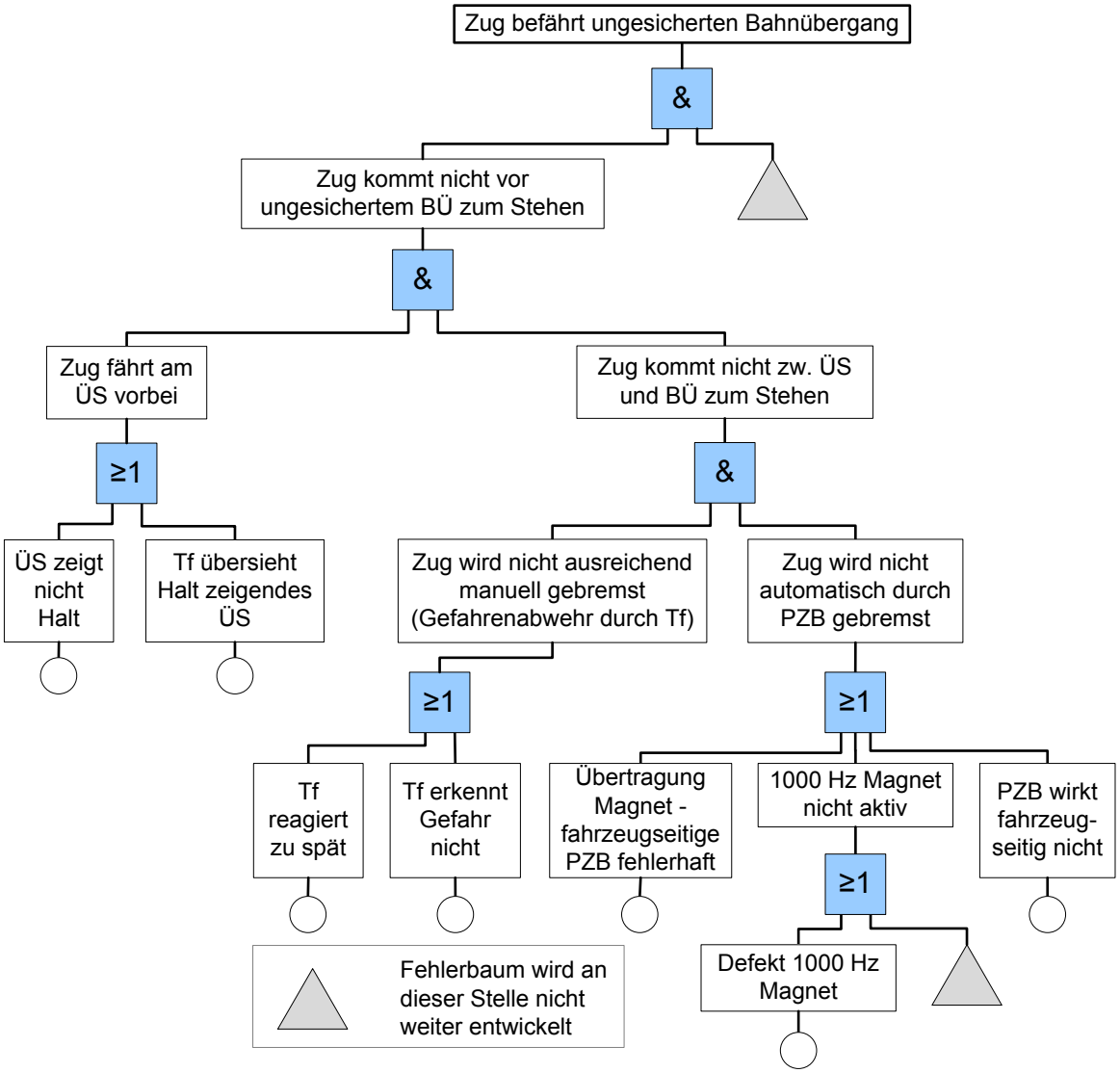

Abbildung 6.5: Ausschnitt aus einem Fehlerbaum für einen Bahnübergang mit Überwachungssignal

Wie an diesem Beispiel zu erkennen ist, ist der Ansatz, als Barrieren die Blätter eines Fehlerbaums zu nehmen, nicht geeignet. Es fehlt demnach noch eine Anleitung, wie Barrieren in Fehlerbäumen identifiziert werden können. Ein Ansatz hierzu wurde bereits in [Sch10] veröffentlicht. Dort werden im Fehlerbaum aus Abbildung 6.5, in dem sieben Blätter vorhanden sind, nur zwei Barrieren identifiziert: PZB und Tf.

Allerdings wird in [Sch10] bereits großer Wert auf die Unabhängigkeit der identifizierten Barrieren gelegt. Harms-Ringdahl und Hollnagel, die angeben, dass Barrieren in Fehlerbäumen einfach zu finden seien, fordern diese Unabhängigkeit nicht. Sie verwenden – wie viele andere – den Begriff Barriere eher lax; ein Umstand, den auch Sklet bemerkt: „almost everything may be considered as a barrier. Therefore it is important to distinguish between the barrier itself that may prevent, control, or mitigate the event sequence or accident scenario directly [...], and the *risk influencing factors* that influence the barrier performance. Examples on risk influencing factors are competence of a third party checker and testing of gas detectors“ [Skl06].
Bei der viel verwendeten weniger rigorosen Definition des Begriffs Barriere kommen weit mehr Elemente eines Fehlerbaums als Barriere in Frage, als wenn man eine strengere Definition verwendet und Unabhängigkeit verlangt. Unabhängigkeit ist wichtig, weil man nur dann, wenn die Barrieren unabhängig voneinander sind, einzelne herausnehmen und durch andere ersetzen kann. Dies ist das Ziel des Ansatzes der Sicherheitsschichten.
Aufgrund der oben gegebenen Argumentation soll im Rahmen dieser Arbeit die Methode verwendet werden, die bereits in [Sch10] vorgestellt wurde, um unabhängige Barrieren in Fehlerbäumen zu identifizieren.

6.4.2 Voraussetzungen

Es liegt ein qualitativer Fehlerbaum für das betrachtete System vor, dessen Top-Ereignis der gewählten Gefährdung entspricht. Der Fehlerbaum ist mindestens bis zur geeigneten Detaillierungstiefe entwickelt worden. Die geeignete Detaillierungstiefe ist vom jeweiligen System, seinen Grenzen, der zu untersuchenden Gefährdung und dem Zweck der Analyse abhängig. Folgende Punkte können als Orientierungshilfe dienen:

- Der Fehlerbaum sollte unterhalb des Top-Ereignisses mindestens zwei, besser drei Ebenen umfassen.
- Der Fehlerbaum sollte mindestens eine ODER-Verknüpfung aufweisen.
- Der Fehlerbaum sollte unterhalb der ersten auftretenden ODER-Verknüpfungen (vom Top-Ereignis aus gesehen) noch ein bis zwei Ebenen weiter entwickelt werden.
- Der Fehlerbaum sollte vom Hersteller nicht weiter entwickelt werden als bis zur Ebene der zugekauften Subkomponenten. Detailliertere Fehlerbäume sollten auf Ergebnissen vom Zulieferer aufbauen.
- Eine Entwicklung des Fehlerbaums bis zu einer Ebene von Relaiskontakten oder einzelnen Schaltkreisen ist in der Regel nicht notwendig.

Um die Analyse mit der ISES-Methode zu erleichtern, sollte jedes Ereignis / jeder Ausfall im Fehlerbaum nur ein Mal vorkommen. Der Fehlerbaum sollte nicht vermascht sein. Bei der Beschreibung der Methode wird im Folgenden davon ausgegangen, dass der Fehlerbaum diese Anforderungen erfüllt.

6.4.3 Durchführung

Ziel des Schritts B und der hier vorgestellten (Teil-)Methode ist es, unabhängige, also hintereinander liegende Sicherheitsbarrieren des Systems aus einem Fehlerbaum zu identifizieren. Die Formulierung „hintereinander liegend“ bezieht sich auf die Darstellung als Schweizer-Käse-Modell (SCM) (Abschnitt 4.6) und damit auf die additive Wirkung der Barrieren.
Für hintereinander liegende Barrieren X und Y im Schweizer-Käse-Modell gilt, dass sowohl X als auch Y durchbrochen werden müssen, damit das unerwünschte Ereignis (der Unfall) eintreten kann. In einem Fehlerbaum müssen daher die Ausfälle der Barrieren, das „Versagen der Barriere X“ und das „Versagen der Barriere Y“, UND-verknüpft sein. UND-Verknüpfungen im Fehlerbaum sind also Hinweise auf hintereinander liegende Barrieren. ODER-Verknüpfungen hingegen beschreiben andere

Mechanismen, z. B. Teile von Barrieren oder verschiedene Arten, wie eine Barriere durchbrochen werden kann.
Um die Barrieren des Bahnübergangs mit Hilfe eines Fehlerbaums zu identifizieren, werden vom Top-Ereignis, der Wurzel des Baumes, aus abwärts in Richtung der Blätter die Verknüpfungen untersucht. Unter einer UND-Verknüpfung werden die Äste des Fehlerbaums weiter betrachtet. ODER-Verknüpfungen sind ein Stopp-Kriterium. Enthält ein Ast eines Fehlerbaums keine ODER-Verknüpfung, sondern nur UND-Verknüpfungen, so ist jedes seiner Blätter ein Hinweis auf vorhandene Barrieren. Enthält ein Ast eine oder mehrere ODER-Verknüpfungen, wird von der Wurzel des Baums ausgehend die erste auftretende ODER-Verknüpfung markiert (siehe Abbildung 6.8, rote Markierungen). Der Ast wird danach nicht weiter untersucht. Stattdessen wird zum nächsten Ast übergegangen. Die Elemente direkt oberhalb und unterhalb dieser ersten ODER-Verknüpfungen geben Hinweise auf die vorhandenen Barrieren.
Unterhalb der ODER-Verknüpfungen sind zwei Fälle zu unterscheiden:

1. Es handelt sich um eine Unterteilung in mehrere Komponenten, die in ihrem Zusammenwirken eine Reihenschaltung darstellen.
2. Es handelt sich um Aktivierung, Funktion und Deaktivierung ein und derselben Komponente.

Die beiden Fälle werden im Folgenden weiter betrachtet.

Fall 1: Komponenten-Reihenschaltung

Bei einer Komponenten-Reihenschaltung besteht die gesuchte Barriere aus mehreren Komponenten, die als logische Reihenschaltung zusammenwirken. Damit die Barriere erfolgreich ihre Funktion erfüllen kann, müssen alle Komponenten aus dieser Reihenschaltung gemäß ihrem Entwurf zusammenwirken. Der Ausfall einer Komponente bedeutet den Ausfall der ganzen Barriere.

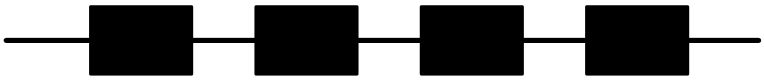

Abbildung 6.6: Reihenschaltung

Stößt man bei der Suche nach Barrieren im Fehlerbaum auf eine solche ODER-Verknüpfung mit darunterliegender Komponenten-Reihenschaltung, kann die Suche an dieser Stelle abgebrochen werden. Die gesuchte Barriere befindet sich im Fehlerbaum über der ODER-Verknüpfung. Sie besteht aus dem Teilsystem, das wiederum aus den Komponenten der Reihenschaltung besteht.

Fall 2: Aktivierung – Funktion – Deaktivierung

Beim 2. Fall, der Aktivierung, Funktion und Deaktivierung, handelt es sich um eine Barriere, die nicht permanent einsatzbereit ist. Sie muss zunächst aktiviert werden, bevor sie ihre Funktion ausüben kann. Sobald sie nicht mehr gebraucht wird, wird sie deaktiviert. Solche Barrieren sind vor allem dort zu finden, wo ihre dauerhafte Aktivierung hemmend auf den Betrieb oder in einer anderen Weise störend wirken würde. Ein Beispiel hierfür ist eine Sprinkleranlage zur Brandbekämpfung in einem Eisenbahnwagen. Ihre dauerhafte Aktivierung würde zwar Brände deutlich erschweren, sie würde aber auch alle Fahrgäste vertreiben und dadurch einen Fahrgastbetrieb unmöglich machen.
Im Fehlerbaum kann sich der Hinweis auf die Barriere nicht nur, wie bei der Reihenschaltung, über der ersten auftretenden ODER-Verknüpfung befinden. Oft findet sich direkt unter dieser ODER-Verknüpfung ein deutlicherer Hinweis auf die Barriere: Es ist das Teilsystem, dessen Aktivierung, Funktion und Deaktivierung in den Ereignissen unter der ODER-Verknüpfung beschreiben wird.
Im Gegensatz zum Fall 1 endet die Suche nach den Barrieren an dieser Stelle des Fehlerbaums noch nicht. Ist unterhalb der ODER-Verknüpfung, in dem Zweig, der das Nicht-Funktionieren der

Barriere behandelt, eine UND-Verknüpfung zu finden, kann die Barriere möglicherweise in mehrere Teil-Barrieren untergliedert werden.

6.4.4 Ergebnis

Die Ergebnisse dieses Schritts sind:

- Ein Fehlerbaum für die betrachtete Gefährdung des zu untersuchenden Systems, in dem alle ersten auftretenden ODER-Verknüpfungen markiert sind
- Eine Liste mit identifizierten Barrieren aus diesem Fehlerbaum, d. h. eine Liste für die betrachtete Gefährdung

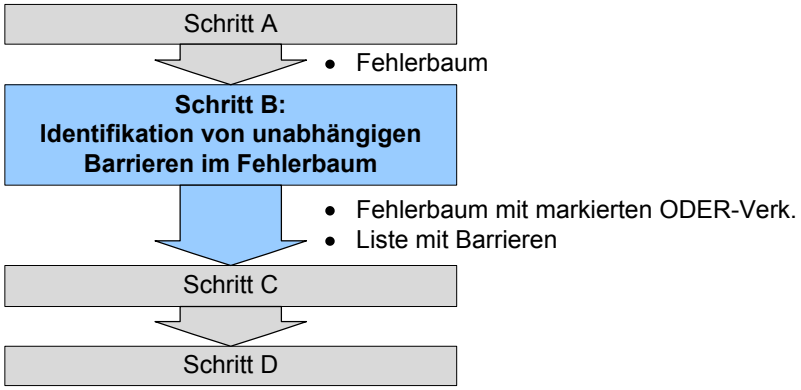

Abbildung 6.7: Schritt B der ISES-Methode

6.4.5 Beispiel

Im Fehlerbaum für das Beispiel einer Geschwindigkeitsüberwachung aus Abbildung 6.4 sollen unabhängige, hintereinander liegende Sicherheitsbarrieren identifiziert werden. Ausgehend vom Top-Ereignis werden die ersten auftretenden ODER-Verknüpfungen gesucht und markiert (siehe Abbildung 6.8).

Fall 1: Komponenten-Reihenschaltung

Eine erste ODER-Verknüpfung, unter der sich eine Reihenschaltung befindet, ist in Abbildung 6.8 auf der linken Seite zu sehen. Die ODER-Verknüpfung befindet sich unter dem Fehlerereignis „Manuelle Geschwindigkeitsüberwachung funktioniert nicht / Zug zu schnell“. Unter der ODER-Verknüpfung befinden sich Fehlerereignisse der Komponenten der manuellen Geschwindigkeitsüberwachung: des Tf und des Tachometers. Der Tf ist für die Geschwindigkeit des Zuges zuständig. Um die Geschwindigkeit richtig regeln zu können, braucht der Tf den Tachometer, der ihm die aktuelle Geschwindigkeit anzeigt. Damit die manuelle Geschwindigkeitsüberwachung richtig funktionieren kann, müssen sowohl der Tf als auch der Tachometer fehlerfrei arbeiten. Damit ist die gesuchte Barriere die *manuelle Geschwindigkeitsüberwachung*.

Fall 2: Aktivierung – Funktion – Deaktivierung

Eine erste ODER-Verknüpfung, unter der sich der Fall Aktivierung – Funktion – Deaktivierung befindet, ist in Abbildung 6.8 unter dem Fehlerereignis „Technische Geschwindigkeitsüberwachung funktioniert nicht / Zug wird nicht gebremst“ zu sehen. Dieses Ereignis kann dadurch verursacht werden, dass die technische Geschwindigkeitsüberwachung

- Nicht eingeschaltet wird (Aktivierung),

- Zwar eingeschaltet wird, aber nicht ordnungsgemäß funktioniert (Funktion) oder
- Bereits (wieder) ausgeschaltet wurde (Deaktivierung)

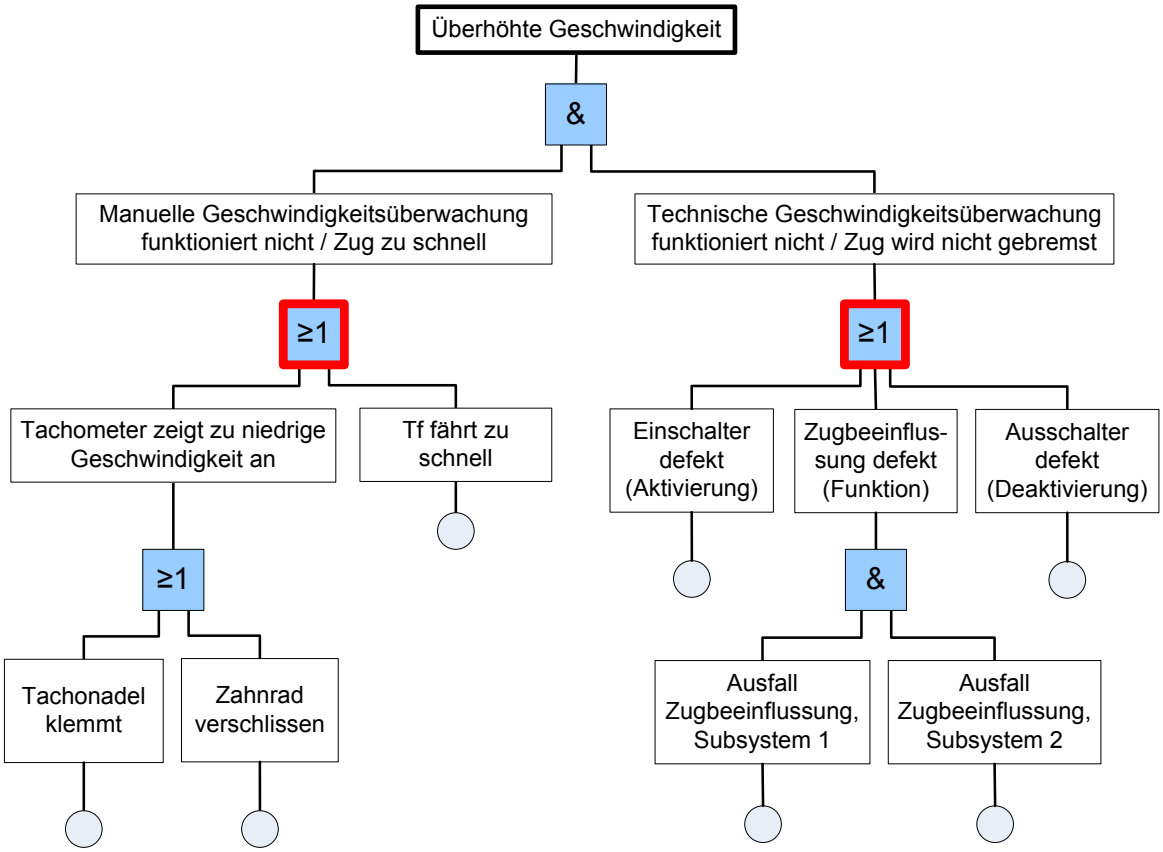

Abbildung 6.8: Beispiel-Fehlerbaum mit markierten ersten ODER-Verknüpfungen

Die gesuchte Barriere befindet sich unter der ODER-Verknüpfung: die Zugbeeinflussung. Sie ist namentlich im Fehlerbaumelement für die Funktion, unterhalb der ODER-Verknüpfung, aufgeführt. Direkt unter dem Fehlerereignis für die Funktion, „Zugbeeinflussung defekt“, befindet sich eine UND-Verknüpfung. Hier kann die Barriere mit Hilfe des Fehlerbaums in additive Teilbarrieren zerlegt werden – bis zu einer weiteren ODER-Verknüpfung oder, wie hier, bis zum Ende des Baumes. Die additiven Teilbarrieren sind *Zugbeeinflussung, Subsystem 1* und *Zugbeeinflussung, Subsystem 2*.
Anhand des Fehlerbaums wurden folgende Barrieren für das Beispiel-System zur Geschwindigkeitsüberwachung aus Abbildung 6.4 identifiziert:

- Manuelle Geschwindigkeitsüberwachung
- Zugbeeinflussung, Subsystem 1
- Zugbeeinflussung, Subsystem 2

6.4.6 Bewertung

Durch die hier beschriebene Methode lassen sich in einem Fehlerbaum enthaltene, unabhängige Barrieren identifizieren. Diese Barrieren sind in ihrer Wirkung additiv. Sie müssen alle ausfallen, bevor das Top-Ereignis des Fehlerbaums eintreten kann.
Die identifizierten Barrieren sind zwar voneinander unabhängig, es sind jedoch noch keine Sicherheitsschichten: Zu einer Sicherheitsschicht gehört neben der Barriere auch die Funktion, und das Barriere-Funktions-Paar muss neben den Unabhängigkeitskriterien auch das Wirksamkeitskriterium erfüllen (Abschnitt 3.2).
Erstellen verschiedene Personen Fehlerbäume für dasselbe Top-Ereignis, so sehen diese Fehlerbäume in der Regel leicht unterschiedlich aus. Wie auch bei logischen Gleichungen gibt es keine richtige

oder falsche Darstellung. Es gibt lediglich vollständige oder unvollständige Fehlerbäume. Sind zwei unterschiedlich aussehende Fehlerbäume für ein System (in Bezug auf einen bestimmten Detaillierungsgrad) vollständig, so enthalten beide jeweils alle Barrieren, die im Fehlerbaum dargestellt werden können. Es ist zu erwarten, dass durch das oben beschriebene Vorgehen in beiden Fällen die gleichen Barrieren identifiziert werden.
Die Methode zur Identifikation von Barrieren im Fehlerbaum ist nicht schwieriger als die FTA selbst: Der Schwierigkeitsgrad ist durchschnittlich bis anspruchsvoll – je nach betrachtetem System.

6.5 Schritt C: Identifikation von Barriere-Funktions-Paaren mit Hilfe von Checklisten

Das *Ziel* des Schritts C ist es, mit Hilfe von Checklisten die Barrieren, die in Schritt B mit Hilfe der Fehlerbaumanalyse identifiziert wurden, zu ergänzen und zu vervollständigen. Es werden die zugehörigen Funktionen identifiziert und so Barriere-Funktions-Paare (B-F-Paare) gebildet. Ein weiteres Ziel dieses Schritts ist es, die Ergebnisse so aufzubereiten, dass sie für nachfolgende Analysen wiederverwendbar sind.

6.5.1 Situation

Checklisten sind ein beliebtes Mittel, um wiederkehrende, ähnliche Tätigkeiten zu vereinfachen und den Bearbeiter zu unterstützen. Sie dienen vor allem folgenden Zwecken:

- Vergleichbarkeit herstellen (Tätigkeiten laufen immer gleich ab)
- Arbeitserleichterung: Tätigkeit kann auch von weniger geübten Personen durchgeführt werden
- Speichern von Wissen aus vorangegangenen Projekten
- Gewährleisten, dass nichts vergessen wird
- Gewährleisten, dass Vorgaben (z. B. Normen) erfüllt werden

Die DIN EN 50129 [DIN03] listet Checklisten als Maßnahme zur Qualitätssicherung und zur Unterstützung in verschiedenen Lebenszyklusphasen. Eine Checkliste zur Identifikation von Barrieren und Funktionen bzw. Sicherheitsschichten in Eisenbahnsystemen ist derzeit noch nicht verfügbar. Die technischen Komponenten eines Systems sind seinem Hersteller jedoch bekannt. Allerdings weiß der Hersteller nicht immer, welche technischen Komponenten seines Systems *Barrieren* enthalten. Die Arbeit mit *(Sicherheits-)Funktionen* wird zwar von den CENELEC-Normen gefordert, stößt in der Praxis jedoch immer noch auf Schwierigkeiten, insbesondere dann, wenn nur kleine, abgegrenzte Teilsysteme betrachtet werden. Es existieren Listen von Funktionen, z. B. in der E DIN EN 15380-4 [DIN09], die jedoch weit mehr als nur Sicherheitsfunktionen enthalten.
Die Barriereanalyse (Abschnitt 5.5) verwendet Checklisten zur Identifikation von Energiequellen und Barrieren (Implementierung von Barrieremechanismen). Die Barriereanalyse ist eine gut bekannte, für Sicherheitsanalysen in verschiedenen Bereichen verwendete Methode. Allerdings wird sie im Bereich der Eisenbahn noch kaum verwendet. Daher sind für den Eisenbahnbereich noch kaum entsprechenden Checklisten vorhanden.
Nur im Bereich der Prävention von Suiziden mit Hilfe der Eisenbahn wurde von Rådbo et al. eine Checkliste erstellt (siehe [RSA08]). Die Erstellung dieser Checkliste erfolgte nicht formal mit Hilfe der Barriereanalyse. Vielmehr wurden Haddons ursprüngliche zehn Strategien (siehe Abschnitt 4.2) als Basis für ein nicht näher beschriebenes Vorgehen verwendet. Dabei wurde diese Checkliste so spezifisch auf das Problem der Suizide zugeschnitten, dass sie auch Barrieren enthält, die dem Betrieb der Eisenbahn entgegen stehen. Beispielsweise wird vorgeschlagen, den Eisenbahnverkehr einzustellen. Aufgrund dieses sehr spezifischen Anwendungsbereichs kann die Checkliste von Rådbo et al. nicht als Basis für das Eisenbahnsystem dienen.

Um die Barriereanalyse im Eisenbahnbereich anzuwenden, bedarf es daher zunächst einer neuen, auf die Eisenbahn angepassten Checkliste, die für die Analyse als Basis verwendet und anschließend weiterentwickelt werden kann.
Die Kombination von Barrieren aus einer Fehlerbaumanalyse (FTA) und Barrieren auf Basis von Haddons zehn Strategien wird auch bei Rådbo et al. [RSA08] verwendet. Allerdings dienen dort sowohl die FTA als auch Haddons Strategien der Identifikation von *möglichen* Barrieren zur künftigen Vermeidung von Suiziden mit Hilfe der Eisenbahn. Das Ziel ist es dabei nicht, ein existierendes System zu modellieren, sondern theoretische Vermeidungsmaßnahmen zur Reduzierung von Suiziden zu entwickeln – sogar ohne dabei die Realisierbarkeit zu prüfen: „Further empirical research is needed to establish their practical feasibility." [RSA08]. Daher ist die Arbeit von Rådbo et al. eher als Sammlung zu verstehen, die alle Ideen (ungeachtet ihrer Realisierbarkeit) umfasst. Dem entsprechend ergeben sich für Rådbo et al. keine Anforderungen, nicht evtl. zu viele Barrieren zu identifizieren.

Basis-Checkliste für den Bereich Eisenbahn

Da Risiko- und Sicherheitsanalysen bei der Eisenbahn meist zielgerichtet in Bezug auf einzelne Gefährdungen durchgeführt werden, wie z. B. im Rahmen der SIRF [EBVVD12], stellt sich die Frage, ob die Checklisten für die ISES-Methode auf einzelne Gefährdungen ausgerichtet werden sollten. Für jede Gefährdung eine eigene Checkliste zu haben, hätte den Vorteil, dass diese Checkliste relativ kurz und damit übersichtlich und leicht handhabbar wäre. Ein Nachteil dieser gefährdungsbezogenen Checklisten wäre, dass Barrieren, die gegen verschiedene Gefährdungen wirken, in allen entsprechenden Checklisten wiederholt werden müssten. Dabei entstünde zusätzlicher Aufwand, und es bestünde die Gefahr von Inkonsistenzen. Ebenso kann es vorkommen, dass der Ersteller der Checklisten die Wirksamkeit einer Barriere gegen eine bestimmte Gefährdung nicht erfasst, wodurch die entsprechende Checkliste unvollständig würde. Fehlt eine bereits im System vorhandenen Barriere in der Checkliste für eine relevante Gefährdung, so kann das dazu führen, dass dem System unnötigerweise eine weitere Barriere hinzugefügt wird, wodurch unnötige Kosten entstehen würden.
Es ist eine Aufgabe der Checklisten, den Fokus der Betrachtung zu erweitern und den Analysten auf Gedanken zu bringen, die er bisher nicht hatte – sei es aus Gewohnheit, aus einem zu engen Blickwinkel heraus, aufgrund seiner Ausbildung oder anderen Gründen. Durch eine gemeinsame Checkliste für alle Gefährdungen kann diese Aufgabe besser erfüllt werden als durch getrennte Checklisten für einzelne Gefährdungen. Daher wird von Checklisten, die auf einzelne Gefährdungen zugeschnitten sind, abgeraten. Stattdessen wird im Folgenden eine Checkliste verwendet, die Funktionen und Barrieren gegen verschiedene Gefährdungen enthält.
Die Energieart, die bei der Eisenbahn von besonderer Bedeutung ist, ist die kinetisch-lineare Energie. Die wichtigsten Ziele[2], die bei der Eisenbahn vor ungewolltem Energiefluss geschützt werden sollen, sind Menschen: Fahrgäste, Personal und Straßenverkehrsteilnehmer. Von den zwölf in [Eri05] genannten Strategien zum Kontrollieren gefährlicher Energieflüsse und zum Schutz der Ziele sind die in Tabelle 6.1 genannten für die Eisenbahn besonders relevant. Zu diesen ausgewählten Strategien enthält Tabelle 6.1 Beispiele für Barrieren, die diese Strategien umsetzen. Dazu wurden die in [Eri05] aufgeführte Liste mit Strategien und ihren Umsetzungen als Basis verwendet. Die Umsetzungen der Strategien aus [Eri05] wurden auf die Eisenbahn angepasst und ergänzt. Um den funktionalen Ansatz der CENELEC-Normen zu berücksichtigen und mit Hinblick auf das Ziel, Sicherheitsschichten zu identifizieren, wurde die ursprüngliche Liste erweitert: Zwischen den Strategien und ihrer Umsetzung durch Barrieren wurden die zugehörigen Funktionen ergänzt. Diese Funktionen sind konkreter als Strategien, die auch als Kategorien von Funktionen interpretiert werden können, aber genereller als die Umsetzungen. Während eine Funktion noch lösungsneutral ist, bezeichnet die Barriere bereits eine mögliche Umsetzung der Funktion mit Hilfe von physischen und / oder nicht-physischen Mitteln (Abschnitt 3.2.2). Die konkreten Mittel, die zur Umsetzung von Funktio-

[2] Personen oder Gegenstände, siehe auch Abschnitt 5.5

nen eingesetzt werden, werden auch als Ressourcen bezeichnet (z. B. im Bereich der Prozessindustrie und der Automatisierungstechnik, siehe [Sch99]). Die Ressource instanziiert die Funktion [Sch09]. Es ist zu beachten, dass eine Ressource nicht technischer Natur sein muss – auch der Mensch kann als Ressource betrachtet werden. Ebenso können nicht-physische Mittel als Ressourcen betrachtet werden. Damit korrespondiert die Unterscheidung zwischen Funktion und Ressource sowie die Zuordnung von Funktion und Ressource mit dem Konzept Funktion – Barriere, wobei Barrieren eine bestimmte Art von Ressourcen bezeichnen: solche, die geplant wurden, um unerwünschte Ereignisse oder Unfälle zu vermeiden, zu beherrschen oder abzumildern (siehe Abschnitt 3.2.2).
Je nach Bedarf können Funktionen auch in Subfunktionen unterteilt werden. Auf diese Weise kann der Detaillierungsgrad der Analyse den Bedürfnissen der Anwender angepasst werden. Wenn Subfunktionen verwendet werden, sollten diese den Funktionen zugeordnet werden. Auf diese Weise kann das Ergebnis der Analyse auf verschiedenen Ebenen genutzt werden.

Tabelle 6.1: Basis-Checkliste zur Bestimmung von Barriere-Funktions-Paaren für den Bereich Eisenbahn

Strategie	**Funktion**	**Barriere / Umsetzung, Bsp.**
1. Reduzieren der Energie menge	Fahrzeuggeschwindigkeit reduzieren	Geschwindigkeitsbeschränkung (durch Schilder oder Signale), Geschwindigkeitsüberwachung / Zugbeeinflussung
2. Trennung von Energie und Ziel in Zeit und / oder Raum	betriebliche Regeln aufstellen	betriebliche Regeln zum Abstand Halten (Zugleitbetrieb, StVO)
	Reihenfolge festlegen	Vorfahrtsregeln (StVO)
	Wartepositionen festlegen	Signale und Tafeln im Bahnhof
	Arbeit so gestalten, dass das Ziel nicht so nah an die Energiequelle heran muss	Bedienung per Fernsteuerung (Rangieren)
	Wege freigeben / verwehren	(Licht-)Signalanlagen installieren (Hauptsignale, Überwachungssignale, etc., auch in Kombination mit Zugbeeinflussung; Lichtzeichen für den Straßenverkehr am BÜ)
	betreten von Gleisanlagen verbieten	Verkehrsregeln (StVO)
	energiegeladene Gegenstände außer Reichweite von Personen halten	hohe Elektrifizierung / Oberleitungen
	Ausweichmöglichkeiten / Fluchtmöglichkeiten bieten	Halbschranken
	Verkehrswege trennen	zweites Gleis
	BÜ entfernen	Umbau
	Neubau von BÜ verhindern	Bauvorschriften, Baupläne
3. Isolierung durch Einfügen materieller Barrieren	Umgebung gestalten	Topographie des Geländes, stabile Hülle (Steifigkeit des Wagenkastens), unterirdische Verkabelung, Gehäuse von Bahnanlagen
	Gefahrenbereich absperren	Absperrungen, Schranken

Tabelle 6.1: Basis-Checkliste zur Bestimmung von Barriere-Funktions-Paaren für den Bereich Eisenbahn (Fortsetzung)

Strategie	Funktion	Barriere / Umsetzung, Bsp.
4. Verändern von Oberflächen, an denen man sich verletzen kann	abrunden von Ecken und Kanten	abgerundete Sitzkanten, Griffe
	weichmachen von Kontaktflächen	schaumstoffummantelte Stangen, gepolsterte Sitze, Gummikanten an Türen
5. Stärken des Ziels, um der Energie standzuhalten	Schutzkleidung tragen	Handschuhe
6. Schulung von Menschen zum Verhindern, dass Energie freigesetzt wird	informieren, warnen	Warnschilder (Signaltafeln, Andreaskreuze, Baken)
	unterrichten, Regeln aufschreiben und zugänglich machen, spezielle Prozeduren / Notfallmaßnahmen schulen	spezielle Prozeduren (z. B. Fahrdienstvorschrift, Straßenverkehrsordnung)
	üben	Sicherheitstraining (Ausbildung der Tf, Fahrschule)

In Abbildung 6.9 ist dargestellt, wann die in Tabelle 6.1 aufgeführten Strategien in einem Unfallverlauf wirken. Die Darstellung ist angelehnt an die von Kjellen [Kje00], wurde jedoch für den Eisenbahnbereich angepasst.

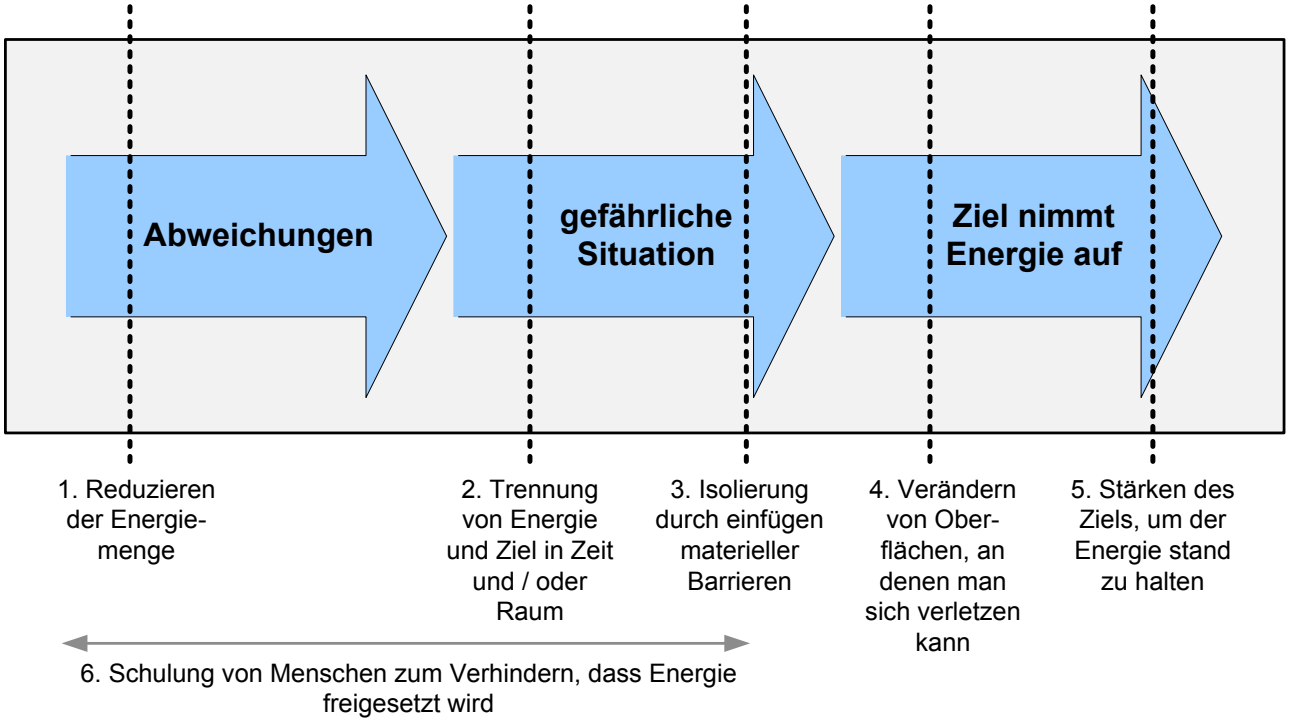

Abbildung 6.9: Strategien aus dem Eisenbahnbereich und ihre Wirkung in einem Unfallverlauf

6.5.2 Voraussetzungen

Schritt B ist abgeschlossen und es liegt für die zu betrachtende Gefährdung eine Liste mit den identifizierten Barrieren aus dem entsprechenden Fehlerbaum vor.
Als Arbeitsmittel werden bereits vorhandene Checklisten genutzt, die Strategien, Funktionen und Barrieren / Umsetzungen von Barrieremechanismen enthalten. Existiert noch keine Checkliste, kann als Basis die Checkliste aus Tabelle 6.1 verwendet werden.

6.5.3 Durchführung

Beim Arbeiten mit Checklisten gibt es stets drei Aspekte:

1. Vorbereitung der Checklisten
2. Nutzung der Checklisten
3. Ergänzung der Checklisten

C1: Vorbereitung der Checklisten

Im Schritt C werden nach Möglichkeit bereits vorhandene Checklisten genutzt. Diese Checklisten können z. B. aus anderen Projekten stammen. Bevor diese Checklisten genutzt werden, sollten sie daraufhin überprüft werden, ob sie aktuell und in Bezug auf das betrachtete System / Gefährdung möglichst vollständig sind. Ebenso sollte geprüft werden, ob sie auf der richtigen Detaillierungsebene (z. B. Funktionen, Subfunktionen etc.) vorliegen.
Insbesondere, wenn die Analyse für ein System oder eine Gefährdung durchgeführt werden soll, das noch nicht in ähnlicher Form betrachtet wurde, ist es notwendig, die Checklisten zu überarbeiten. Hierzu können verschiedenen Quellen verwendet werden. Zunächst wählt man sich eine bereits existierende Checkliste als Basis. Falls noch keine geeignete Checkliste vorhanden ist, kann als Grundlage die Basis-Checkliste aus Tabelle 6.1 verwendet werden.
Anschließend werden geeignete Informationsquellen zur Überarbeitung gesucht. Dies können z. B. Gesetze sein, die für das System bestimmte Arten der Implementierung vorschreiben, z. B. die Eisenbahn-Bau- und Betriebsordnung (EBO) [Bun12]. Ebenfalls in Frage kommen Dokumente, die Sicherheitsfunktionen für das betrachtete System oder ein ähnliches / generisches System beschreiben. In den Informationsquellen wird nach Barrieren und Funktionen gesucht. Dabei kann das Ergebnis einer solchen Suche – je nach verwendeter Dokumentation – sehr unterschiedlich sein. Bevor neue Einträge in die Checkliste aufgenommen werden, wird geprüft, ob entsprechende B-F-Paare in den Listen bereits enthalten sind. Doppelte Eintragungen sind zu vermeiden. Ist die gefundene Barriere oder Funktion wirklich neu, wird sie (falls notwendig und möglich) zu einem B-F-Paar ergänzt. Anschließend werden Barriere und Funktion einer Strategie zugeordnet und an entsprechender Stelle in die Checkliste eingetragen.

C2: Nutzung der Checklisten

Ausgehend von den in Schritt B (Abschnitt 6.4) identifizierten Barrieren werden mit Hilfe der Checklisten die zugehörigen Funktionen bestimmt. Ist für eine vorhandene Barriere keine passende Funktion in den Checklisten enthalten, so wird eine entsprechende Funktion ergänzt. Dabei wird die Funktion einer Strategie (siehe Tabelle 6.1) zugeordnet. Auch die identifizierten Barrieren werden als Umsetzung von Barrieremechanismen den Checklisten hinzugefügt – und dabei ihren Funktionen zugeordnet. Dabei können Barrieren durchaus doppelt auftreten, wenn sie mehrere Barrieremechanismen oder mehrere Funktionen umsetzen.
Anschließend werden die Checklisten verwendet, um festzustellen, ob bei der durchgeführten FTA Barrieren oder Funktionen übersehen wurden. Barrieren können z. B. übersehen werden, wenn das betrachtete System zu klein gewählt wurde, oder dadurch, dass für eine bestimmte Gefährdung keine

FTA durchgeführt wurde. Für diese Prüfung werden die Strategien, Funktionen und Barrieren aus den Checklisten durchgegangen.
Für jede Strategie wird gefragt: Wird diese Strategie im betrachteten System verwendet? Wenn ja, mit Hilfe welcher Funktionen? Falls die Funktionen zu diesem Zeitpunkt schwer zu bestimmen sind, kann auch direkt nach den Barrieren gefragt werden. Die Funktionen können dann aus den Barrieren abgeleitet werden.
Für jede Funktion wird gefragt: Ist diese Funktion im betrachteten System implementiert? Wenn ja, durch welche Barrieren? Wie wird die Funktion umgesetzt?
Als Basisdokumentation kann hierbei ein Systementwurf, eine tatsächliche Implementierung des Systems (Hardware / Software) oder eine Anforderungsspezifikation (Lastenheft) dienen. Bei der Nutzung von Systementwürfen und Anforderungsspezifikationen muss allerdings geprüft werden, ob die geforderten Funktionen auch tatsächlich umgesetzt wurden.

C3: Ergänzung der Checklisten

Das Ergänzen der Checklisten dient dem Zweck, nachfolgende Analysen zu erleichtern. Einmal erworbene Erkenntnisse werden festgehalten, sodass sie auch in Zukunft zur Verfügung stehen. Kreativ Barrieren und Funktionen zu identifizieren ist schwieriger, als sie anhand von Checklisten zu finden. Dieselben Barrieren und Funktionen bei der 2., 3., 4. Analyse wieder und wieder kreativ zu identifizieren, ist zeitraubend, fehleranfällig und unnötig. Daher wird folgendes Verfahren angewandt:
Wurden während einer Analyse neue Barrieren, Funktionen oder womöglich auch Strategien identifiziert, so werden diese den Checklisten hinzugefügt. Es können auch andere Quellen herangezogen werden, um Checklisten zu ergänzen, z. B. Ergebnisse aus anderen Projekten oder Funktionslisten wie z. B. die E DIN EN 15380-4 [DIN09] für Fahrzeuge, die allerdings sowohl sicherheitsrelevante als auch nicht-sicherheitsrelevante Funktionen beinhaltet. Eine solche Funktionsliste kann nicht direkt in eine Checkliste übernommen werden. Sie muss zunächst bereinigt werden, denn in die Checklisten dürfen nur sicherheitsrelevante Funktionen aufgenommen werden. Ferner müssen die Funktionen den Strategien zugeordnet und nach Möglichkeit um Barrieren ergänzt werden. Diese Arbeit kann sehr aufwändig sein und man enthält als Ergebnis wahrscheinlich auch Funktionen, die für die aktuelle Analyse gerade nicht von Belang sind, sie erhöht aber den Vollständigkeitsgrad der Checklisten.

6.5.4 Ergebnis

Ein Ergebnis des Schritts C ist die Liste mit den identifizierten Barrieren-Funktions-Paaren für die betrachtete Gefährdung, wie z. B. „Zugbeeinflussung – Geschwindigkeit reduzieren“.

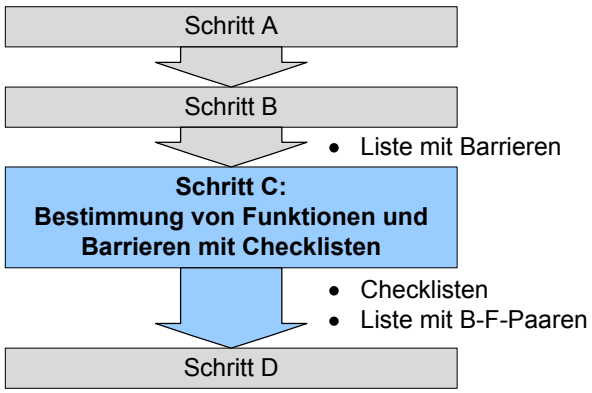

Abbildung 6.10: Schritt C der ISES-Methode

Ein weiteres Ergebnis sind die Checklisten mit Strategien, Funktionen und Barrieren / Umsetzungen von Barrieremechanismen (siehe auch Abbildung 6.10). Diese Checklisten können speziell auf das

zu untersuchende (generische) System zugeschnitten sein.

Falls vor der Durchführung von Schritt C bereits Checklisten vorhanden waren, besteht das Ergebnis aus den erweiterten und aktualisierten Checklisten für den Eisenbahnbereich. Die Checklisten dienen sowohl der Dokumentation der Analyse als auch als Basis für zukünftige Analysen.

6.5.5 Beispiel

Im Schritt C werden für das Beispiel die Funktionen bestimmt, die zu den mit Hilfe der FTA identifizierten Barrieren gehören (siehe Abschnitt 6.4.5). Anschließend wird mit Hilfe der Checklisten nach weiteren Barrieren im Beispiel-System gesucht. Werden in diesem Schritt Lücken in den Checklisten entdeckt, dann werden die Checklisten entsprechend ergänzt.

Vorbereitung der Checklisten

Als Arbeitsmittel für das Beispiel wird die Basis-Checkliste aus Tabelle 6.1 verwendet. Auf die Vorbereitung der Checkliste wird an dieser Stelle aus Gründen der Übersichtlichkeit verzichtet. Ein ausführliches Beispiel zur Vorbereitung von Checklisten findet sich in Kapitel 9.

Nutzung der Checklisten

Die Basis-Checkliste wird zunächst dazu genutzt, für die in Schritt B bestimmten Barrieren die zugehörigen Funktionen zu bestimmen. Die beiden Subsysteme der Zugbeeinflussung entsprechen der Umsetzung *Geschwindigkeitsüberwachung / Zugsicherung*. Die zugehörige Funktion ist *Fahrzeuggeschwindigkeit reduzieren*.

Die manuelle Geschwindigkeitsüberwachung gehört ebenfalls zum Punkt *Geschwindigkeitsüberwachung / Zugsicherung*. In der Checkliste (Tabelle 6.1) fehlt allerdings in der Spalte Umsetzung die Variante manuell, d. h. der Triebfahrzeugführer. Bisher ist dort nur die technische Umsetzung dieser Funktion aufgeführt. Der Tf wird daher zur Ergänzung der Checkliste vorgemerkt.

Anmerkung: Im Fehlerbaum ist neben dem Tf auch der Tachometer enthalten (siehe Abbildung 6.8). Der Tf ist aber der eigentlich Ausführende. Selbstverständlich benötigt der Tf als Barriere immer Hilfsmittel, wie z. B. den Tachometer oder einen Fahr-Brems-Hebel. Um die Bezeichnung für die Barriere kurz zu halten, wird in der Tabelle als abkürzende Schreibweise nur der Tf aufgeführt anstatt von der Barriere „Tf + Tachometer + Fahr-Brems-Hebel + X + Y + Z“ zu sprechen.

Nachdem die Funktionen der Barrieren bestimmt wurden, wird mit Hilfe der Checklisten nach weiteren, bisher noch nicht identifizierten Barrieren und Funktionen im Beispiel-System gesucht. Eine Barriere, die im System enthalten ist, aber nicht in der FTA identifiziert wurde, ist die *Geschwindigkeitsbeschränkung*. Ohne eine Geschwindigkeitsbeschränkung gäbe es für den Tf keinen Anlass, die Geschwindigkeit des Zuges unter einem bestimmten Wert zu halten. In der Checkliste Tabelle 6.1 sind als Umsetzung für die Geschwindigkeitsbeschränkung Schilder oder Signale angegeben. Zum betrachteten Beispiel-System gehören jedoch weder Schilder noch Signale, dennoch wird diese Funktion umgesetzt. Das bedeutet, hier ist die Checkliste unvollständig. Der Tf, der unter Zuhilfenahme des Tachometers die Geschwindigkeit unterhalb der erlaubten Geschwindigkeit halten soll, tut dies aufgrund seines Wissens, seiner Kenntnis von der Geschwindigkeitsbeschränkung. Dieses Wissen entstammt einer Vorschrift, z. B. dem Buchfahrplan. Diese Barriere wird zusammen mit ihrer Funktion zur Liste der Barriere-Funktions-Paare des Beispiel-Systems hinzugefügt. Die Liste der für das Beispiel identifizierten Barriere-Funktions-Paare ist in Tabelle 6.2 dargestellt.

Tabelle 6.2: Identifizierte Barriere-Funktions-Paare für das Beispiel

Strategie	Funktion	Barriere / Umsetzung	Nr.
1. Reduzieren der Energiemenge	Fahrzeug-geschwindigkeit reduzieren	Geschwindigkeitsbeschränkung (durch Vorschriften, z. B. Buchfahrplan)	1
		Geschwindigkeitsüberwachung / Zugbeeinflussung (manuelle Geschwindigkeitsüberwachung, Triebfahrzeugführer)	2
		Geschwindigkeitsüberwachung / Zugbeeinflussung (Zugbeeinflussung, Subsystem 1)	3
		Geschwindigkeitsüberwachung / Zugbeeinflussung (Zugbeeinflussung, Subsystem 2)	4

Ergänzung der Checklisten

Nach der Identifikation der Barriere-Funktions-Paare werden in der Checkliste die fehlenden Barrieren und Funktionen ergänzt, um für die nächste Analyse eine bessere Arbeitsgrundlage zu haben. Aus Platzgründen wird die ergänzte Checkliste an dieser Stelle nicht noch einmal abgedruckt.

6.5.6 Bewertung

Das Arbeiten mit Checklisten ist relativ einfach, da der Analyst strukturiert zu den wichtigen Fragen geführt wird. Mögliche Antworten (Funktionen, Barrieren) sind bereits vorgegeben, der Analyst muss nur noch auswählen und ggf. die Formulierung etwas anpassen. Durch die vorgegebenen Strategien, Funktionen und Barrieren wird der Analyst gelenkt, sodass es im leichter fällt, den richtigen Detaillierungsgrad zu treffen und auch fehlende oder gar neue Funktionen und Barrieren mit einzufügen.
Die Vorbereitung der Checklisten kann sehr aufwändig sein, wenn für das analysierte System noch keine geeignete Checkliste zur Verfügung steht. Je mehr Quellen für die Vorbereitung der Checklisten herangezogen werden, desto höher ist der Arbeitsaufwand. In gleichem Maße steigt aber auch die Qualität der Checklisten, was bei ihrer Nutzung und späteren Ergänzung zu einer Arbeitserleichterung führt. Der Grad der Vollständigkeit der Analyseergebnisse ist abhängig von der Qualität der Checklisten. Daher ist es ratsam, einen gewissen Arbeitsaufwand in Kauf zu nehmen.
Die Arbeit mit vorhandenen Checklisten birgt jedoch auch die Gefahr, dass sich der Analyst zu sehr auf die Vollständigkeit und Korrektheit der Checklisten verlässt. Daher bedarf es in diesem Schritt einer sorgfältigen Prüfung der Ergebnisse. Ein „Scheuklappen-Verhalten“ muss unbedingt vermieden werden, denn sonst könnten zu wenige oder falsche B-F-Paare identifiziert werden.

6.6 Schritt D: Prüfen auf Wirksamkeit und Unabhängigkeit

Das *Ziel* des Schritts D ist es, die in Schritt C identifizierten Barriere-Funktions-Paare (B-F-Paare) bzgl. der Kriterien für Sicherheitsschichten (Wirksamkeit, Unabhängigkeit) zu prüfen und dadurch die Sicherheitsschichten zu identifizieren.

6.6.1 Situation

Unabhängigkeit ist im Bereich der Eisenbahn ein wichtiges Prinzip zur Gewährleistung der Sicherheit eines Systems. Nur wenn Einheiten voneinander unabhängig sind, „addieren“ sie sich in ihrer Wir-

kung. Nur bei unabhängigen Einheiten kann davon ausgegangen werden, dass ein Ausfall einer Einheit nicht auch zu einem Ausfall der anderen Einheiten führt und damit ein Dominoeffekt bei vermeintlich hintereinander liegenden Barrieren eintritt. Die Analyse der Unabhängigkeit von Betrachtungseinheiten ist im Bereich der Eisenbahn tief verwurzelt und Bestandteil jedes Sicherheitsnachweises gemäß DIN EN 50129 [DIN03].
Bereits bei der Fehlerbaumanalyse spielt die Unabhängigkeit von Einheiten oder Komponenten eine wichtige Rolle. Nur unabhängige Ereignisse dürfen im Fehlerbaum durch ein UND-Gatter verknüpft werden.
Ein weiterer Aspekt der Unabhängigkeit ist, dass die Unabhängigkeit von Einheiten die Berechnungen bzgl. Ausfall- oder Gefährdungsraten erleichtert. Unabhängigkeit hat den Vorteil, dass man dadurch die Ausfall- oder Gefährdungsraten eines Systems mitunter beträchtlich senken kann.

6.6.2 Voraussetzungen

Voraussetzung für Schritt D ist, dass Schritt C abgeschlossen wurde und für jede betrachtete Gefährdung eine vollständige Liste mit identifizierten Barrieren-Funktions-Paaren vorliegt. Diese Vollständigkeit wurde durch den Abgleich mit den Checklisten in Schritt C geprüft.

6.6.3 Durchführung

In diesem Schritt werden die B-F-Paare darauf überprüft, ob sie den Kriterien für Sicherheitsschichten bzgl. Wirksamkeit und Unabhängigkeit genügen.

Wirksamkeit

Die Frage nach der Wirksamkeit (Abschnitt 3.2.4) wird zweckmäßigerweise zuerst gestellt. Ein B-F-Paar muss, um eine Sicherheitsschicht sein zu können, gegen das betrachtete unerwünschte Ereignis wirksam sein. Es muss zudem das Eintreten des unerwünschten Ereignisses allein verhindern können. Um dies zu prüfen, werden gedanklich alle anderen identifizierten B-F-Paare aus dem System entfernt bzw. als fehlerhaft, d. h. als nicht erfolgreiche Maßnahme, betrachtet. Das zu prüfenden B-F-Paar selbst wird hingegen als frei von zufälligen Fehlern angenommen. Systematische Schwächen des B-F-Paars werden jedoch bei der Prüfung berücksichtigt. In dem so betrachteten Szenario wird geprüft, ob das B-F-Paar in der Lage ist, das Eintreten des betrachteten unerwünschten Ereignisses zu verhindern. Reduziert das zu prüfende B-F-Paar nur die Folgen des unerwünschten Ereignisses (z. B. die Unfallschwere), dann gilt dies nicht als wirksam gegen das unerwünschte Ereignis.
Eine erste Prüfung der Wirksamkeit kann oft schon anhand der Strategie erfolgen, der das B-F-Paar zugeordnet ist. Es gibt Strategien, die gegen einige Ereignisse nicht wirksam sein können. Z. B. kann die Strategie 4 „Verändern von Oberflächen, an denen man sich verletzen kann“ zwar die Folgen eines Aufpralls eines Fahrgasts auf eine Haltestange abmildern, aber den Aufprall / den Sturz selbst kann sie nicht verhindern.
Ist die Strategie prinzipiell geeignet, gegen das unerwünschte Ereignis erfolgreich eingesetzt zu werden, müssen alle B-F-Paare dieser Strategie einzeln auf ihre Wirksamkeit geprüft werden. Dabei kann der Vergleich mit anderen identifizierten B-F-Paaren hilfreich sein, um Unterschiede in der Wirkungsweise der einzelnen Barrieren zu erkennen.
Ist ein B-F-Paar nicht gegen das betrachtete unerwünschte Ereignis wirksam, kann es keine Sicherheitsschicht sein. Dennoch müssen auch nicht wirksame B-F-Paare bei der Prüfung der Unabhängigkeitskriterien berücksichtigt werden, da hierdurch Abhängigkeiten zwischen den B-F-Paaren aufgedeckt werden können. Ein nicht wirksames B-F-Paar kann zwar keine Sicherheitsschicht bilden, es kann jedoch ggf. Teil einer Sicherheitsschicht sein.

Unabhängigkeit

Nach der Frage der Wirksamkeit wird die Unabhängigkeit der B-F-Paare geprüft. Ein B-F-Paar ist unabhängig von allen anderen B-F-Paaren des betrachteten Systems (im Hinblick auf die betrachtete Gefährdung), wenn die Unabhängigkeitskriterien aus Abschnitt 3.2.5 gelten:

a) Die Funktion des B-F-Paars ist keine (echte) Teilfunktion eines anderen B-F-Paars.
b) Die Barriere des B-F-Paars ist kein Teil einer Barriere eines anderen B-F-Paars.
c) Es ist nicht die Funktion des B-F-Paars, ein anderes B-F-Paar zu aktivieren oder zu deaktivieren.
d) Die Barriere des B-F-Paars ist nicht in der Lage, durch eine Fehlfunktion oder einen Ausfall eine Barriere eines anderen B-F-Paars zu deaktivieren oder in einer anderen Weise in ihrer Wirksamkeit zu beeinträchtigen.
e) Die Barriere des B-F-Paars teilt kein technisches Betriebsmittel mit einer Barriere eines anderen B-F-Paars.

Identifikation der Sicherheitsschichten

Genügen Barriere-Funktions-Paare aus Schritt C diesen Unabhängigkeitskriterien und dem Wirksamkeitskriterium, so sind diese Barriere-Funktions-Paare die gesuchten Sicherheitsschichten. Genügt ein B-F-Paar einem oder mehreren Kriterien nicht, so ist es keine Sicherheitsschicht. Es ist jedoch möglich, dass es zu einem anderen B-F-Paar gehört und mit diesem zusammen eine Sicherheitsschicht bildet. Bei der Prüfung der Kriterien werden in diesem Fall durch die identifizierten Abhängigkeiten zwischen den B-F-Paaren potentielle Partner identifiziert.
Die Prüfung und ihre Ergebnisse werden in Form einer Tabelle dokumentiert (siehe Tabelle 6.3). Dazu werden alle Barriere-Funktions-Paare mit Nummer, Funktion und Barriere untereinander aufgelistet. In den Spalten werden die Ergebnisse der Prüfung notiert, dabei tragen die Spalten die Buchstaben der Kriterien als Überschrift. Für die Bewertung wird folgende Notation verwendet:

\+ Kriterium erfüllt
\- **(Zahl)** Kriterium nicht erfüllt. Die Zahl in Klammern bezeichnet das Barriere-Funktions-Paar, mit dem bzgl. der Unabhängigkeit ein Konflikt besteht. In der Spalte für das Wirksamkeitskriterium wird keine Zahl angegeben.
M Sonderfall Mensch
id (Zahl) Die Funktion / Barriere ist identisch mit der Funktion / Barriere des Barriere-Funktions-Paars, das in Klammern angegeben ist.
n. a. Kriterium ist für dieses Barriere-Funktions-Paar nicht anwendbar.
(Großbuchstabe) Fußnote für weitere Erläuterungen. Statt eines Großbuchstaben kann auch ein beliebiges anderes Symbol verwendet werden, außer kleinen Buchstaben (Unabhängigkeitskriterien) und Zahlen (Barriere-Funktions-Paaren).

Tabelle 6.3: Beispiel für eine Tabelle mit Barriere-Funktions-Paaren zur Prüfung der Kriterien für Sicherheitsschichten

Barriere-Funktions-Paar			Kriterien						gehört
Nr.	Funktion	Barriere	Wirk.	a	b	c	d	e	zu
1	Funktion 1	Barriere 1	+	+	+	+	+	+	
2	Funktion 2	Barriere 2	-	+ id (3)	+	- (1)	+	+	1
3	Funktion 3	Barriere 3	+	+ id (2)	M	+	M	n. a. (Z)	

Genügt ein B-F-Paar nicht allen Kriterien, so wird in der letzten Spalte – falls möglich – die Nummer des B-F-Paars vermerkt, zu dem es gehört (potentieller Partner). Als potenzielle Partner kommen

dabei zunächst die B-F-Paare in Frage, die durch die Zahlen in Klammern (sofern vorhanden) identifiziert werden. Die Liste der potenziellen Partner ist jedoch nicht auf die aufgeführten Zahlen in Klammern beschränkt. Dies gilt insbesondere dann, wenn das B-F-Paar das Wirksamkeitskriterium nicht erfüllt.
Bei der Prüfung der Unabhängigkeit werden folgende Regeln angewandt:

- Ist die Funktion des B-F-Paars X eine Teilfunktion des B-F-Paars Y (Kriterium **a**)), dann bilden diese beiden B-F-Paare zusammen eine Sicherheitsschicht mit der Funktion des B-F-Paars Y.
- Ist die Barriere des B-F-Paars X ein Teil der Barriere des B-F-Paars Y (Kriterium **b**)), dann bilden diese beiden B-F-Paare zusammen eine Sicherheitsschicht mit der Barriere des B-F-Paars Y. Bei der Betrachtung von Teilfunktionen und Teilbarrieren, ist es wichtig, zwischen echten Teilmengen und anderen Common Cause Failures (CCF) wie z. B. einer Aktivierung zu unterscheiden. Während echte Teilmengen eine Abhängigkeit der B-F-Paare bedeuten und somit zu nur einer Sicherheitsschicht führen, bedeuten andere CCF zwei unabhängige Sicherheitsschichten mit einer gemeinsamen Schwäche (siehe auch Abbildung 6.11).

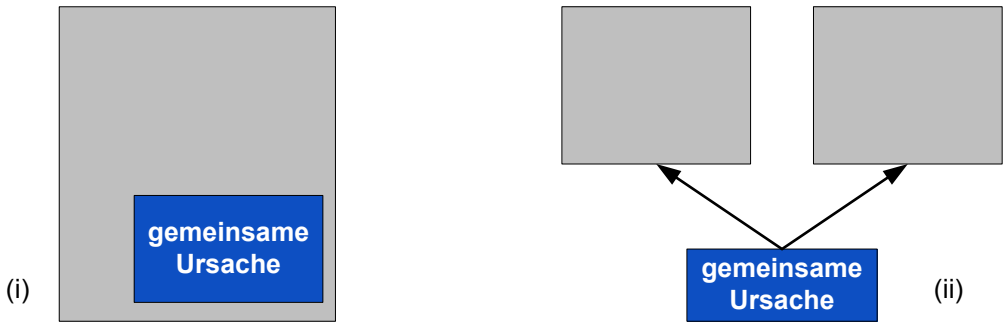

Abbildung 6.11: Unterschied zwischen einer Teilmenge (i) und anderen CCF (ii)

- Ist es die Funktion des B-F-Paars X, das B-F-Paar Y zu aktivieren oder zu deaktivieren (Kriterium **c**)), dann ist das B-F-Paar X keine SiS, sondern eine Schwäche des B-F-Paars Y. Das B-F-Paar X wird bei ggf. einer späteren Bewertung der Sicherheit der Sicherheitsschicht Y (falls Y eine SiS ist) benötigt. Daher lohnt es sich, diese Information an einer geeigneten Stelle zu notieren, um sie später zu verwenden. Dies kann auch in der Tabelle 6.3 geschehen.
- Ist die Barriere des B-F-Paars X in der Lage, durch eine Fehlfunktion oder einen Ausfall die Barriere des B-F-Paars Y zu deaktivieren oder in einer anderen Weise in ihrer Wirksamkeit zu beeinträchtigen (Kriterium **d**)), dann ist das B-F-Paar X keine eigenständige Sicherheitsschicht, sondern gehört zum B-F-Paar Y. X beschreibt dann eine Schwäche von Y.
- Wenn zwei B-F-Paare X und Y dasselbe Betriebsmittel nutzen (Kriterium **e**)), aber zwei verschiedenen Funktionen ausführen, dann müssen diese zwei B-F-Paare zusammengefasst als eine Sicherheitsschicht betrachtet werden.

Die Barrieren der Barriere-Funktions-Paare sind noch generischer Natur, sie sind quasi Barrieretypen. Ihre tatsächliche, spezifische Implementierung (Sklet [Skl06] nennt dies das Barrieresystem) lässt sich erst erkennen, wenn sie als Teil einer Anlage detailliert geplant und gebaut werden. Z. B ist das Barriere-Funktions-Paar: *Signal – Wege freigeben / verwehren* generischer Natur, eine mögliche spezifische Implementierung der Barriere „Signal“ wäre das Überwachungssignal SP200 der Firma PINTSCH BAMAG [PINoJ].
Für Barrieren, die mit Hilfe der Fehlerbaumanalyse identifiziert wurden (Schritt B), ist aufgrund der Methode sichergestellt, dass sie voneinander stochastisch unabhängig sind (vergleiche auch Abschnitt 3.3.1). Das liegt an der Methode FTA. Damit in einem Fehlerbaum zwei Ereignisse mit einem UND verknüpft werden können, müssen sie stochastisch unabhängig sein. Da alle Barrieren, die mit Hilfe der FTA identifiziert wurden, UND-verknüpft sind (bei den ersten auftretenden ODER-

Verknüpfungen wird die Suche abgebrochen, es sei denn es handelt sich um Aktivierung, Funktion und Deaktivierung, siehe Schritt B), sind sie voneinander stochastisch unabhängig. Dadurch erfüllen diese Barrieren bereits die Kriterien **b**), **d**) und **e**). Da jedoch durch die Arbeit mit den Checklisten noch weitere B-F-Paare hinzugekommen sind, sollten auch für die B-F-Paare aus Schritt B alle Unabhängigkeitskriterien **a**) bis **e**) geprüft werden.

6.6.4 Ergebnis

Ein Ergebnis dieses Schritts besteht aus einer Liste mit Sicherheitsschichten für die betrachtete Gefährdung des zu untersuchenden Systems. Diese identifizierten Sicherheitsschichten bilden das Modell der Sicherheitsschichten des Systems – bezogen auf die betrachtete Gefährdung. Ein weiteres Ergebnis ist die Tabelle mit den Ergebnissen der Prüfung der Kriterien für Sicherheitsschichten. Diese Tabelle kann bei späteren CCF-Analysen und bei einer Bewertung der Sicherheit des Systems nützliche Informationen bieten. Mit Schritt D ist die Anwendung der ISES-Methode abgeschlossen (siehe auch Abbildung 6.12).

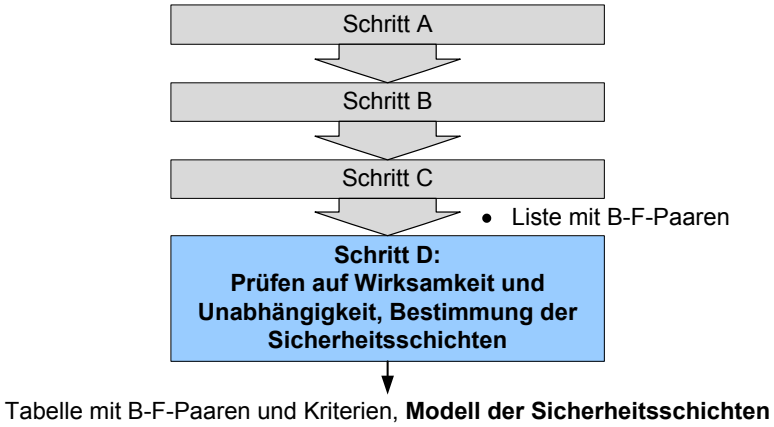

Abbildung 6.12: Schritt D der ISES-Methode

6.6.5 Beispiel

Die Barriere-Funktions-Paare, die für das Beispiel identifiziert wurden (siehe Tabelle 6.2), werden jetzt bzgl. der Kriterien für Sicherheitsschichten analysiert. Das Ergebnis ist in Tabelle 6.4 dargestellt. Die Analyse ergibt, dass ein B-F-Paar die Funktion hat, ein anderes B-F-Paar zu aktivieren oder zu deaktivieren. Die Vorschrift, durch die die Geschwindigkeit beschränkt wird, „aktiviert“ die manuelle Geschwindigkeitsüberwachung. Sie ist der Grund, warum der Triebfahrzeugführer die Geschwindigkeit überwacht. Daher ist das B-F-Paar 1 keine eigenständige Sicherheitsschicht. Es gehört zur manuellen Geschwindigkeitsüberwachung durch den Triebfahrzeugführer, also zum B-F-Paar 2. Damit verbleiben für das Beispiel drei Sicherheitsschichten:

I) Fahrzeuggeschwindigkeit reduzieren – Geschwindigkeitsüberwachung / Zugsicherung (manuelle Geschwindigkeitsüberwachung, Triebfahrzeugführer)
II) Fahrzeuggeschwindigkeit reduzieren – Geschwindigkeitsüberwachung / Zugsicherung (Zugbeeinflussung, Subsystem 1)
III) Fahrzeuggeschwindigkeit reduzieren – Geschwindigkeitsüberwachung / Zugsicherung (Zugbeeinflussung, Subsystem 2)

Die Nummerierung I bis III dient der einfachen und eindeutigen Bezeichnung der Sicherheitsschichten und stellt keine Reihenfolge bzgl. des Wirkens dar. Obwohl das B-F-Paar 1 keine eigenständige

Tabelle 6.4: Prüfung der Kriterien für Sicherheitsschichten für die Barriere-Funktions-Paare des Beispiels

Barriere-Funktions-Paar			Kriterien						gehört
Nr.	Funktion	Barriere	W.	a	b	c	d	e	zu
1	Fahrzeug-geschwin-digkeit reduzieren	Geschwindigkeitsbeschrän-kung (durch Vorschriften)	-	+ id (2, 3, 4)	+	+	n. a.	n. a.	2
2	Fahrzeug-geschwin-digkeit reduzieren	Geschw.-Überwachung / Zugsicherung (manuelle Geschw.-Überwachung, Tf)	+	+ id (1, 3, 4)	M	+	M	n. a.	
3	Fahrzeug-geschwin-digkeit reduzieren	Geschw.-Überwachung / Zugsicherung (Zugbeeinflus-sung, Subsystem 1)	+	+ id (1, 2, 4)	+	+	+	+	
4	Fahrzeug-geschwin-digkeit reduzieren	Geschw.-Überwachung / Zugsicherung (Zugbeeinflus-sung, Subsystem 2)	+	+ id (1, 2, 3)	+	+	+	+	

Sicherheitsschicht darstellt, ist seine Identifikation nicht vergebens gewesen. Dieses B-F-Paar ist ein Teil einer Sicherheitsschicht und wird benötigt, wenn die Qualität und die Sicherheitsleistung dieser Sicherheitsschicht bewertet werden sollen.
Anmerkung: Falls das B-F-Paar 2 durch die Analyse nicht identifiziert worden wäre (z. B. wenn die Barriere in der FTA nicht enthalten gewesen wäre), dann hätte die Identifikation von B-F-Paar 1 einen Hinweis auf dieses fehlende B-F-Paar gegeben.

6.6.6 Bewertung

Die Prüfung der Wirksamkeit eines B-F-Paars verlangt vom Analysten eine sorgfältige Betrachtung. Die Schwierigkeit dieser Prüfung besteht darin, sich von dem Gedanken zu lösen, dass eine Maßnahme, die der Verbesserung der Sicherheit dient, auch eine eigenständige Sicherheitsschicht sein muss. Nicht jede Barriere ist eine Sicherheitsschicht. Ebenfalls besondere Disziplin verlangt es, sich bei der Prüfung der Wirksamkeit auf eine Gefährdung zu konzentrieren. Es mag zunächst schwer fallen, B-F-Paare, die gegen eine Gefährdung wirken, die nicht Gegenstand der Analyse ist, aus der Liste der potenziellen Sicherheitsschichten für die betrachtete Gefährdung zu streichen.
Unabhängigkeitsprüfungen sind oft schwierig, da nicht immer geeignete Kriterien zur Verfügung stehen und damit die Bewertung der Unabhängigkeit zur Ermessenssache wird. Stehen doch Kriterien zur Verfügung, wie z. B. die der stochastischen Unabhängigkeit für UND-Verknüpfungen in einem Fehlerbaum, so sind diese Kriterien bisweilen schwer nachprüfbar (weil z. B. wahrscheinlichkeitstheoretische Überlegungen notwendig wären) oder sie sind so streng, dass sie beinahe nie erfüllt werden (siehe auch Abschnitt 3.3.1).
Mit den Unabhängigkeitskriterien **a**) bis **e**) für Sicherheitsschichten stehen klare Kriterien zur Verfügung, die einzeln geprüft werden können. Einige Unabhängigkeitskriterien lassen sich relativ leicht prüfen, z. B. Kriterium **e**). Bei anderen Kriterien ist es schwieriger. Insgesamt jedoch bewegen sich die Kriterien auf einer geeigneten Ebene: Barrieren und Funktionen. So werden die Anforderungen aus den CENELEC-Normen berücksichtigt und zudem passt diese Ebene zur allgemein üblichen

Vorgehensweise im Eisenbahnbereich: dem Denken in technischen Einheiten und ihren Funktionen. Für jedes B-F-Paar sind insgesamt sechs Kriterien zu prüfen. Dabei kann bei der Wirksamkeitsprüfung mitunter Aufwand gespart werden, indem die zugrundeliegenden Strategien betrachtet werden. Insgesamt ist der Aufwand für die Prüfung umso höher, je mehr potentielle Sicherheitsschichten im Schritt C mit Hilfe der Checklisten zu den ursprünglich identifizierten Barrieren hinzugekommen sind. Die Checklisten dienen der Verbesserung der Vollständigkeit. Dieser Aspekt ist so wichtig, dass er einen gewissen zusätzlichen Aufwand rechtfertigt, denn ein unvollständiges Modell der Sicherheitsschichten eines Systems könnte negative Auswirkungen haben: Die Sicherheit des Systems würde unterschätzt, wodurch Kosten für zusätzliche Sicherheitsmaßnahmen entstehen könnten. Möglicherweise würde das System sogar keine Erlaubnis zur Inbetriebnahme erhalten. Zudem würden mitunter Systemelemente nicht als sicherheitsrelevant erkannt und bei einem Umbau des Systems entfernt und dadurch die Sicherheit des Systems unbeabsichtigt reduziert. Doch auch wenn qualitativ hochwertige Checklisten zu einer Verbesserung der Vollständigkeit der Analyse führen, so dürfen sie doch nicht als Garant für eine Vollständigkeit genommen werden. Sie können den Sachverstand des Analysten nicht ersetzen.
Da die Beschreibung der B-F-Paare insbesondere in den Tabellen in der Regel in knapper Textform erfolgt, besteht die Gefahr, dass Barrieren oder Funktionen falsch bewertet werden, weil der Kontext verloren geht. Hierbei helfen die Strategien, Funktionen und Subfunktionen, die einen Teil des Kontextes enthalten. Es wird jedoch empfohlen, die Beschreibungen der Barrieren und Funktionen nicht zu knapp zu wählen – auch um eine spätere Nachprüfbarkeit der Ergebnisse zu gewährleisten.

7 Regeln und Anwendungshinweise

In diesem Kapitel werden Regeln für die Darstellung von Sicherheitsschichten (SiS) beschrieben sowie nützliche Hinweise für den Umgang mit Sicherheitsschichten und die Anwendung der ISES-Methode gegeben. Diese Regeln und Hinweise sollen dem Anwender des Modells der Sicherheitsschichten und der ISES-Methode Hilfestellung geben, eine Orientierung bieten und das Verständnis vertiefen.

7.1 Zeitpunkt der Anwendung der ISES-Methode

Die in der vorliegenden Arbeit vorgestellte ISES-Methode kann zu verschiedenen Zeitpunkten im Systemlebenszyklus angewendet werden. Sie kann bereits im *Entwurfsstadium* eingesetzt werden, um sich einen Überblick über die geplanten Sicherheitsschichten zu verschaffen. Im Rahmen einer *Risikoanalyse* (Phase 3 „Risikoanalyse“ des Lebenszyklus gemäß DIN EN 50126-1 [DIN00]) identifiziert sie Maßnahmen zur Risikoreduktion. In den Phasen 9 „System-Validierung“ und 10 „Systemabnahme“ des Lebenszyklus gemäß DIN EN 50126-1 [DIN00] kann sie im Rahmen der *Validierung* und *Sicherheitsnachweisführung* eingesetzt werden.
Die ISES-Methode kann auch bei bereits existierenden, sich in Betrieb befindlichen Systemen angewendet werden, z. B. um die *Auswirkungen geplanter Änderungsmaßnahmen* zu beurteilen (Phase 13 „Änderungen und Nachrüstung“ des Lebenszyklus gemäß DIN EN 50126-1 [DIN00]) oder um verschiedene Systeme bzgl. ihres Sicherheitsverhaltens miteinander zu *vergleichen*.
Sie kann sogar nach einem Unfall eingesetzt werden, um die Sicherheitsschichten zu identifizieren, die hätten wirken sollen. Die ISES-Methode kann jedoch nicht eingesetzt werden, um einen Unfallverlauf zu rekonstruieren. Sie ist keine Methode zur Unfallursachenanalyse.

7.2 Darstellung von Sicherheitsschichten

Wie in Kapitel 4 dargelegt, sind Bilder wichtig, um eine Analyse zu unterstützen und ihr Ergebnis verständlicher zu machen. Das *Schweizer-Käse-Modell* ist eine Darstellungsweise, die gut mit dem Fehlerbaum korrespondiert [HWL06], da es die Schwächen von Systemelementen im Hinblick auf ein bestimmtes unerwünschtes Ereignis visualisiert. Außerdem hat das Schweizer-Käse-Modell (SCM) gegenüber den meisten anderen Darstellungsweisen den Vorteil, dass es den Betrachter auch auf die „Löcher im Käse“ aufmerksam macht. Dies ist gerade im Bereich der Sicherheitsanalyse eine enorm wichtige Eigenschaft. Es kann nicht oft genug darauf hingewiesen werden, dass es absolute Sicherheit in der Realität nicht gibt. Fast ebenso wichtig ist es, dass Systementwickler durch die Löcher im Käse dazu angeleitet werden, nicht eine weitere SiS zu entwerfen, die gegen bereits gut abgedeckte Risiken wirkt, sondern zielgerichtet SiS zu entwerfen, die die Schwächen der anderen SiS ausgleichen, oder die Löcher der vorhandenen SiS zielgerichtet zu verkleinern (quasi die Löcher stopfen). Aufgrund dieser positiven Eigenschaften, wird für die Darstellung von Sicherheitsschichten in der vorliegenden Arbeit das Schweizer-Käse-Modell verwendet (siehe auch Abschnitt 4.12). Abbildung 7.1 zeigt die für das Beispiel der überhöhten Geschwindigkeit (Abschnitt 6.6.5) identifizierten Sicherheitsschichten als SCM.
Damit Sicherheitsschichten korrekt im SCM dargestellt werden, müssen einige Regeln beachtet werden, die in den folgenden Abschnitten erläutert werden.

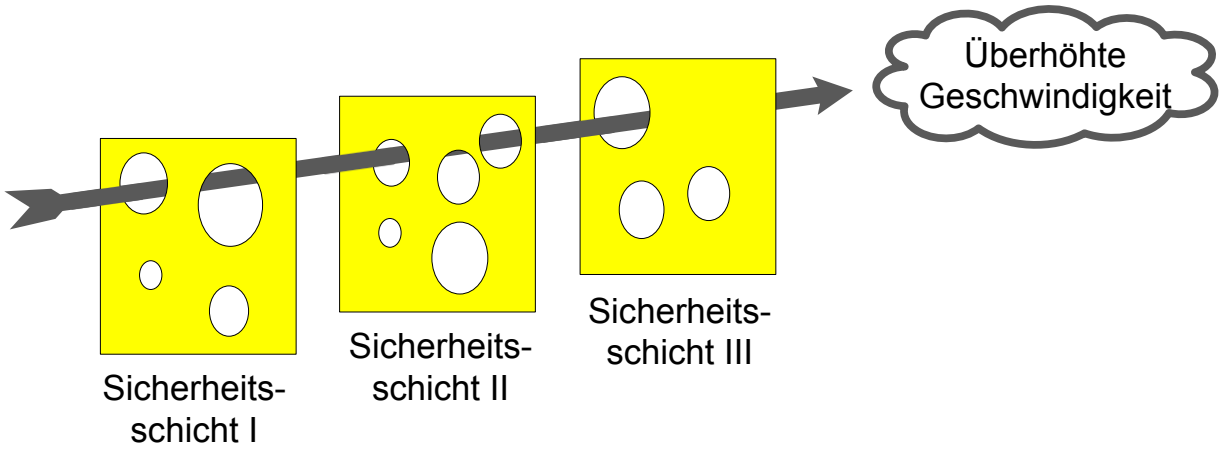

Abbildung 7.1: Sicherheitsschichten als Schweizer-Käse-Modell

7.2.1 Darstellung von Aktivierung und Deaktivierung von Sicherheitsschichten

Es gibt Sicherheitsschichten, deren Barrieren zur Erfüllung ihrer Funktion zunächst aktiviert werden müssen. Ein typisches Beispiel hierfür sind Schranken an Bahnübergängen. Sie sollen ihre schützende Funktion nur in bestimmten Zeiträumen ausüben – immer dann, wenn sich ein Zug nähert. Solche Barrieren werden in der Literatur (z. B. bei Hollnagel [Hol99]) auch aktive Barrieren genannt. Aktivierung und Deaktivierung von Barrieren sind zwei Betrachtungsweisen derselben Eigenschaft: Eine Barriere, die für 5 Minuten pro Stunde aktiviert wird, kann auch betrachtet werden als eine Barriere, die für 55 Minuten pro Stunde deaktiviert wird.

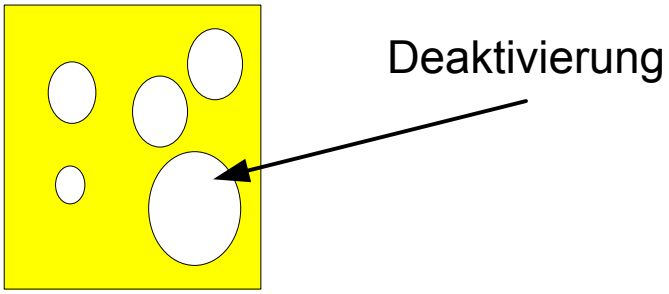

Abbildung 7.2: Darstellung einer deaktivierbaren Sicherheitsschicht im Schweizer-Käse-Modell

Aktive Barrieren bedürfen einer besonders sorgfältigen Betrachtung, weil sie im Gegensatz zu passiven Barrieren (z. B. einer Wand) relativ leicht funktionsunfähig gemacht werden können – sei es durch einen technischen Defekt (Ausfall) oder durch bewusste Deaktivierung zur Arbeitserleichterung bis hin zu Sabotage[1]. Bei der Behandlung und Darstellung solcher Barrieren drängt sich der Eindruck auf, dass diese Barrieren nur zeitweise vorhanden sind. Versucht man dieses zeitabhängige Vorhandensein zu modellieren, stoßen viele Modelle schnell an ihre Grenzen oder werden zunehmend kompliziert.
Wird eine Barriere aus einem System entfernt, so wird damit auch die zugehörige Sicherheitsschicht entfernt. Will man die Aktivierung / Deaktivierung einer Sicherheitsschicht im SCM durch Entfernen der Käsescheibe modellieren, so lässt sich dies ohne bewegte Bilder kaum mehr darstellen. Einfacher und modellgerechter ist es hingegen, die Aktivierung durch das Hinzufügen der Barriere in das Modell und die mögliche Deaktivierung als ein Loch in der Käsescheibe darzustellen (siehe Abbildung 7.2).

[1] Sabotage wird durch Sicherheitsmaßnahmen aus dem Bereich der *security* bekämpft. Der Fokus der vorliegenden Arbeit liegt jedoch auf dem Bereich *safety* (siehe Abschnitt 2.2). Daher werden Aspekte wie Sabotage nicht weiter betrachtet.

Denn eine deaktivierte Barriere verschwindet nicht wirklich aus dem System – sie ist auch in deaktiviertem Zustand stets vorhanden. Z. B. stehen die Schranken eines Bahnübergangs in deaktiviertem Zustand senkrecht, sind aber dennoch vorhanden und sogar sichtbar.

7.2.2 Unterschied zwischen eigenständigen Sicherheitsschicht und einem „Lochstopfer“

Bei der Arbeit mit Checklisten, Schritt C der ISES-Methode, kommen zur Liste der Barrieren mitunter solche hinzu, die zwar die Sicherheit des Systems verbessern, aber zusammen mit ihrer Funktion noch keine eigenständige Sicherheitsschicht bilden. Diese Barrieren dienen dazu, die Leistungsfähigkeit einer anderen Sicherheitsschicht zu verbessern. Ein Beispiel für solche Barrieren sind Schilder, die die Aufmerksamkeit der Menschen auf einen bestimmten Sachverhalt lenken. Schilder erinnern an Regeln oder weisen auf Barrieren hin, damit diese nicht übersehen werden und dadurch nicht wirken können. Für eine Darstellung im SCM macht es scheinbar keinen Unterschied, ob diese „Lochstopfer“-Barrieren als eigene Käsescheibe dargestellt werden oder ob durch ihr Vorhandensein ein Loch einer Käsescheibe verkleinert wird. Allerdings haben diese Barrieren eine Eigenschaft, die dazu führt, dass sie nicht als eigenständige Käsescheibe dargestellt werden dürfen: Sie sind von einer anderen Sicherheitsschicht *abhängig*. Wird die Sicherheitsschicht entfernt, die sie verbessern, verlieren auch die „Lochstopfer“-Barrieren ihre Wirksamkeit. Dies wird durch die Kriterien für Sicherheitsschichten aus Abschnitt 3.2 aufgedeckt. Daher müssen solche Barrieren wie in Abbildung 7.3 dargestellt werden.

Beispiel: Ein Bahnübergang verfügt über Schranken, die verhindern, dass ein Zug und ein Straßenfahrzeug auf dem Bahnübergang zusammenprallen. Schranken sperren die gesamte Straßenbreite, sodass Fahrzeuge auf dem Bahnübergang eingeschlossen werden können. Dies ist ein „Loch“ in der Sicherheitsschicht. Eine Gefahrraumfreimeldung (z. B. durch Personal oder ein Radar) kann dieses „Loch stopfen“. Würde man die Schranken entfernen, würde auch die Gefahrraumfreimeldung ihre Wirkung verlieren, denn solange nicht durch die Schranken garantiert werden kann, dass der Gefahrraum frei bleibt, ist die Gefahrraumfreimeldung wirkungslos.

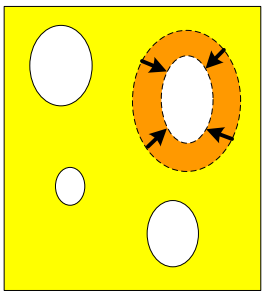

Abbildung 7.3: Darstellung einer „Lochstopfer“-Barriere im Schweizer-Käse-Modell

7.2.3 Kombination von Sicherheitsschichten

Es gibt zwei grundsätzliche Arten, wie Systemelemente funktional miteinander verbunden sein können: das logische Parallelmodell und das logische Serienmodell. Um zu vermeiden, dass es bei der Erstellung oder Interpretation von Schweizer-Käse-Modellen zu Missverständnissen kommt, wird im Folgenden beschrieben, wie diese beiden grundsätzlichen Arten korrekt modelliert werden.

Logisches Parallelmodell

Eine logisches Parallelmodell in einem Zuverlässigkeitsblockdiagramm (ZBD) stellt funktionale Redundanz dar (siehe z. B. [BÖ6] oder [DIN94]). In einem logische Parallelmodell werden Erfolgspfade dargestellt: Ein System ist so lange funktionsfähig, wie mindestens einer der Wege intakt ist (anschauliches Beispiel: elektrischer Strom fließt, ein Ausfall einer Komponente unterbricht die entsprechende Leitung). In einem Fehlerbaum entspricht ein Parallel-Zuverlässigkeitsblockdiagramm einer UND-Verknüpfung. UND-verknüpfte Elemente müssen alle ausfallen, damit es zu einem Ausfall des Gesamtsystems kommt. UND-verknüpfte Sicherheitsschichten müssen alle durchbrochen werden, damit es zu einem Unfall kommen kann. Abbildung 7.4 zeigt, wie Elemente eines logischen Parallelmodells im Schweizer-Käse-Modell dargestellt werden.

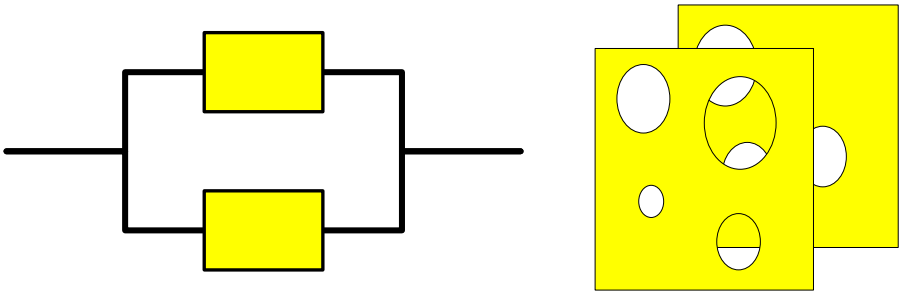

Abbildung 7.4: Logisches Parallelmodell als Zuverlässigkeitsblockdiagramm und im Schweizer-Käse-Modell

Logisches Serienmodell

Ein logisches Serienmodell in einem Zuverlässigkeitsblockdiagramm stellt ein System dar, bei dem alle Komponenten intakt sein müssen, damit das System seine Funktion erfüllen kann (siehe z. B. [MP03]). Alle Komponenten liegen auf dem einzigen Erfolgspfad des Systems. Wie auch beim logischen Parallelmodell kann auch beim Serienmodell elektrischer Strom als anschauliches Beispiel dienen: Ein Ausfall einer Komponente unterbricht die Leitung. Daher wird das logische Serienmodell auch oft als Reihenschaltung bezeichnet. In einem Fehlerbaum entspricht ein Serien-Zuverlässigkeitsblockdiagramm einer ODER-Verknüpfung. Bei ODER-verknüpften Elementen genügt es, wenn ein einziges Element ausfällt, damit es zu einem Ausfall des Gesamtsystems kommt. Aber auch, wenn alle Elemente gemeinsam ausfallen, kommt es zu einem Ausfall des Gesamtsystems.

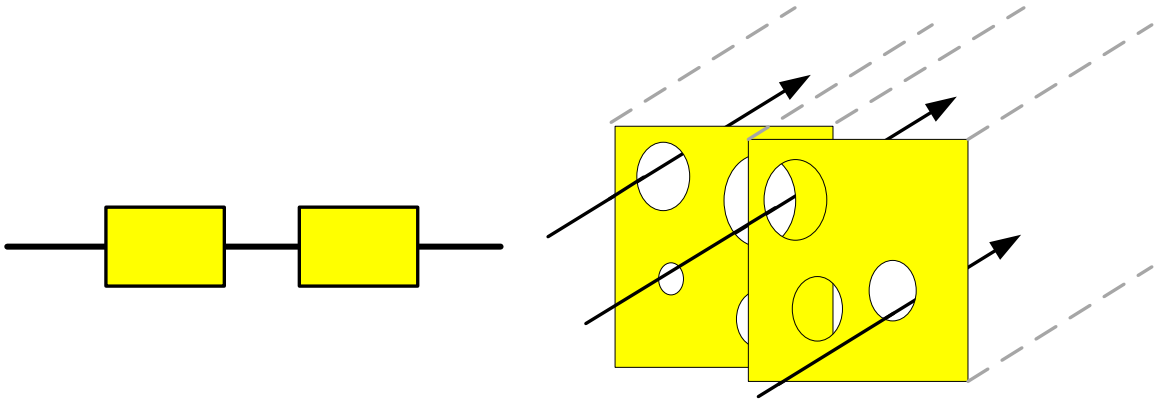

Abbildung 7.5: Logisches Serienmodell als Zuverlässigkeitsblockdiagramm und im Schweizer-Käse-Modell

Im Schweizer-Käse-Modell ist eine ODER-Verknüpfung nicht ganz einfach darzustellen. Es muss verschiedene Pfade durch die Käsescheiben geben: solche, die nur durch eine Käsescheibe führen und solche, die durch alle Käsescheiben führen. Abbildung 7.5 zeigt, wie Elemente, die eine logische Reihenschaltung bilden, im Schweizer-Käse-Modell dargestellt werden können.
Im Modell der Sicherheitsschichten kommt dieses Darstellungsproblem nicht vor, denn im Modell gibt es keine ODER-verknüpften Sicherheitsschichten. Das Modell ist so aufgebaut, dass der Ausfall einer einzelnen Sicherheitsschicht nicht ausreicht, um zu einer Gefährdung zu führen (sofern das System mindestens zwei Sicherheitsschichten besitzt). Besitzt ein System zwei Barrieren, die in einem Fehlerbaum ODER-verknüpft sind, so werden diese beiden Barrieren zu einer Sicherheitsschicht zusammengefasst, sofern für diese resultierende Sicherheitsschicht die in Abschnitt 3.2 aufgeführten Kriterien erfüllt sind. Um jedoch einer falschen Anwendung des SCM vorzubeugen und die Betrachtung der logischen Modelle zu vervollständigen, sei an dieser Stelle auch auf die korrekte Umsetzung eines logischen Serienmodells hingewiesen.

7.3 Modell und Methode bei mehreren Gefährdungen

Die ISES-Methode aus Kapitel 6 identifiziert Sicherheitsschichten für einzelne Gefährdungen. Für ein betrachtetes System gibt es in der Regel jedoch mehr als nur eine Gefährdung. Um mehrere Gefährdungen zu betrachten, muss die ISES-Methode für jede Gefährdung einzeln angewendet werden. Das entspricht dem üblichen Vorgehen bei der Sicherheitsnachweisführung, bei dem der Nachweis der Erfüllung der Sicherheitsanforderungen (THR, Sicherheitsintegritätslevel (SIL)) ebenfalls für einzelne Gefährdungen oder sicherheitsrelevante Funktionen durchgeführt wird. Die Ergebnisse können sowohl einzeln als SCM als auch alle zusammen in einer Graphik dargestellt werden. Ein Beispiel für eine gemeinsame Darstellung von Sicherheitsschichten für mehrere Gefährdungen eines Systems ist in Abbildung 7.6 zu sehen. Bei der Darstellung sollte darauf geachtet werden, Sicherheitsschichten, die gegen mehrere Gefährdungen eingesetzt werden, entsprechend zu kennzeichnen. Auf diese Weise wird verhindert, dass der Eindruck entsteht, das System hätte mehr Sicherheitsschichten als es tatsächlich hat. Diese Kennzeichnung vereinfacht es außerdem, die Folgen eines Entfernens einer Sicherheitsschicht zu erkennen: Erhöht sich dadurch das Risiko bzgl. einer Gefährdung oder gleich bzgl. mehrerer Gefährdungen?

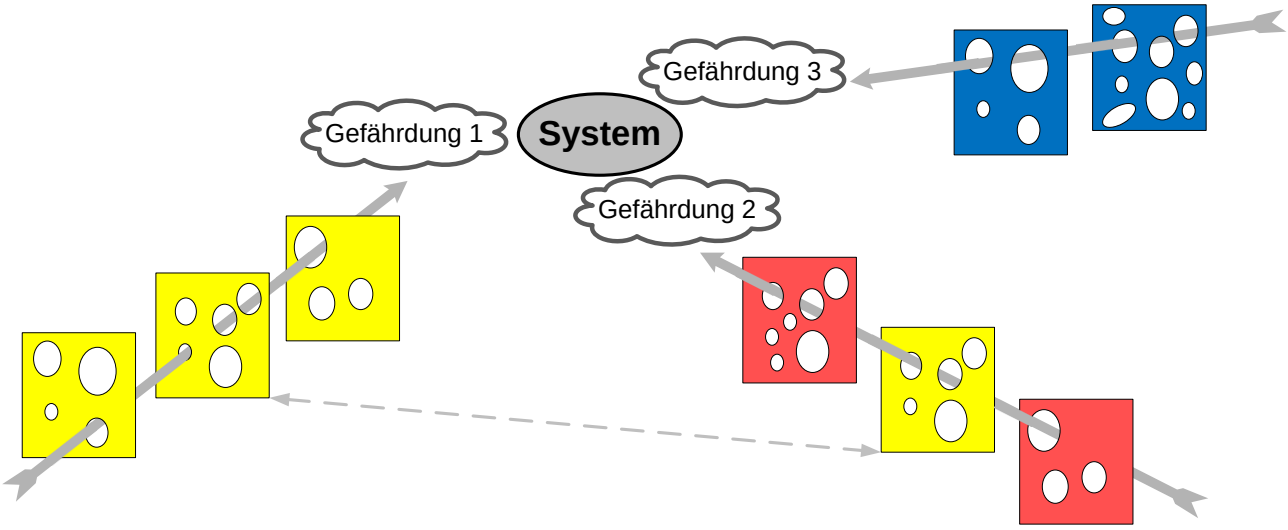

Abbildung 7.6: Mehrere Gefährdungen für ein System: Darstellung als Schweizer-Käse-Modell, eine der gelben Sicherheitsschichten wird gegen zwei Gefährdungen verwendet

Ergänzend zur graphischen Darstellung als SCM kann in Anlehnung an die Hazard-Barrier-Matrix aus [NHDF96] eine Gefährdungs-Sicherheitsschichten-Matrix verwendet werden, um die Ergebnisse

Tabelle 7.1: Gefährdungs-Sicherheitsschichten-Matrix

Gefährdung	SiS 1	SiS 2	SiS 3	SiS 4	SiS 5
Gefährdung 1	+		+		
Gefährdung 2		+	+	+	+
Gefährdung 3	+	+			+

übersichtlich zusammenzufassen. In den Zeilen der Gefährdungs-Sicherheitsschichten-Matrix werden die einzelnen Gefährdungen notiert, in den Spalten stehen alle für das System identifizierten Sicherheitsschichten. Durch Kreuze wird gekennzeichnet, welche Sicherheitsschichten gegen welche Gefährdungen zum Einsatz kommen (siehe Tabelle 7.1).

7.4 Über das Glück

Reason erzählt in [Rea08] von einem Flugzeug, das während eines Fluges durch beinahe unvorstellbares Pech, durch Bauteilversagen, alle drei hydraulischen Systeme gleichzeitig verlor. Der Verlust aller hydraulischen Systeme war für das Flugzeug fatal, damit war es fast nicht mehr manövrierbar. Dennoch gelang es dem Piloten, eine Bruchlandung durchzuführen, bei der ein Großteil der Menschen an Bord des Flugzeugs überlebte. Zwei Faktoren machten dies möglich: die hervorragenden Fähigkeiten des Piloten und *Glück*. Glück, dass der Pilot ein Hobby-Segelflieger war. Glück, dass der Ausfall der hydraulischen Systeme über flachem Land und bei ungewöhnlich ruhigem Wetter erfolgte. Glück, dass durch den besonderen Tag und die Tageszeit außergewöhnlich viele Rettungskräfte am Boden zur Verfügung standen.
Glück vermag Schaden zu reduzieren oder gar Unfälle ganz zu verhindern, obwohl eine Situation eingetreten ist, in der alle Schutzmaßnahmen, alle Barrieren und alle Sicherheitsschichten versagt haben. Eine Situation, in der ein Schaden geradezu eintreten muss, aber doch nicht eintritt.
Die Glücks-Schicht ist die Schicht, die immer da ist, auf die man sich aber nie verlassen sollte, da ihre Löcher zahlreich und extrem mobil sind. Man darf sie weder für Berechnungen noch für die Sicherheitsnachweisführung verwenden. Wozu braucht man sie dann? Sie vervollständigt das Modell. Sie erklärt, warum es manchmal doch keinen Unfall gibt, obwohl alle modellierten Barrieren / Schichten durchbrochen wurden. Sie stellt den Unterschied zwischen Risiko und Gewissheit dar. Schlicht ausgedrückt: Sie modelliert die Modellierungsungenauigkeit.
Im Projekt ROSA wird Glück durchaus modelliert und auch quantifiziert, in Form von sogenannten „Neutralising Factors“ [GHS+09]. Dies mag auf der Ebene des gesamten Eisenbahnnetzes eines Landes, wie es in ROSA betrachtet wird, notwendig sein, um unnötig schlechte (zu konservative) Abschätzungen des Risikos zu vermeiden, ist für den konkreten Einzelfall aber mit Vorsicht zu betrachten. Was man durchaus tun kann, ist z. B. die Verkehrsdichte (Fahrzeuge pro Stunde) zu berücksichtigen, damit die Wahrscheinlichkeiten für Kollisionen anzupassen (ist kein anderer Verkehrsteilnehmer da, kann man auch nicht mit ihm zusammenstoßen) und entsprechend die Sicherheitsmaßnahmen anzupassen. Allerdings fällt dieses Glück eher in den Bereich messbarer Daten und Statistik.

7.5 Methoden zur Bewertung von Sicherheitsschichten

Sicherheitsschichten – als Teil eines sicherheitsrelevanten Systems – müssen früher oder später einer *Bewertung* unterzogen werden. Idealerweise geschieht eine erste grobe Bewertung bereits in der Planungsphase. Eine (vorläufig) abschließende Bewertung erfolgt meist mit der Erstellung des Sicherheitsnachweises, der Begutachtung und der behördlichen Zulassung.

7.5.1 Qualitative und quantitative Methoden

Für die Bewertung der Sicherheit von Systemen gibt es zwei grundsätzliche Arten der Analyse: *qualitative* und *quantitative* Analyse. Außerdem gibt es Mischformen dieser beiden grundsätzlichen Arten, die dann als *semi-quantitativ* bezeichnet werden. Die Frage, welche Art der Bewertung die Beste ist, wird im Bereich der Eisenbahn immer wieder intensiv diskutiert. Bislang ist man noch nicht zu einer Einigung gekommen – es gibt Befürworter für beide Seiten. Braband gibt in [Bra02] eine Auflistung bekannter qualitativer und quantitativer Methoden zur Sicherheitsanalyse. Viele quantitative Methoden lassen sich auch qualitativ einsetzen. Zu diesen Methoden gehören z. B. die Fehlerbaumanalyse (FTA) (Abschnitt 5.6) und die Ereignisbaumanalyse (ETA) (Abschnitt 5.7).
Sowohl qualitative als auch quantitative Methoden haben ihre Vor- und Nachteile. Da *qualitative* Methoden häufig einfacher zu erlernen, durchzuführen und zu verstehen sind als quantitative, werden sie gern verwendet, sind weit verbreitet und gemeinhin akzeptiert. Ein Nachteil der qualitativen Methoden ist, dass sie vorwiegend auf Erfahrungen in bestimmten Anwendungsbereichen beruhen und meist nicht auf eine nachvollziehbare Weise konstruiert wurden. Auch wurde beobachtet, dass die klassischen qualitativen Methoden häufig zu sehr konservativen Ergebnissen, d. h. zu unnötig hohen Sicherheitsanforderungen oder zu einer zu schlechten Einschätzung der Systemsicherheit führen. [Bra05b].
Quantitative Methoden hingegen haben meist das Problem einer schwachen Datengrundlage. Für diese Methoden werden Ausfallraten oder Ausfallwahrscheinlichkeiten von Systemkomponenten benötigt. Diese Werte sind bei der zuverlässigen Technik, die im Bereich der Eisenbahn eingesetzt wird, meist so klein, dass sie im Laborexperiment nicht in entsprechend kurzer Zeit bestimmt werden können. Dies gilt insbesondere dann, wenn nur eine geringe Anzahl der Systemkomponenten hergestellt / eingesetzt wird. Alternativ versucht man, die notwendigen Informationen in Form von Felddaten zu erfassen, aber häufig gestaltet sich der Rückfluss der Erfahrungen der Betreiber an den Hersteller als schwierig. Eine weitere Schwäche quantitativer Analysen ist, dass sie – unreflektiert angewendet – den Analysten zu vermeintlich hochpräzisen Aussagen führen (z. B. „die Ausfallrate dieses Systems beträgt $2,834 \cdot 10^{-17}/h$ “). Diesem Ergebnis gegenüber stehen Eingangswerte, die bei weitem nicht so genau sind. Ein Vorteil der quantitativen Methoden ist hingegen, dass sie die Sicherheit unterschiedlicher Systeme vergleichbar machen, und neue Wege für eine objektivere Risikoakzeptanz öffnen.
Entscheidend für die Wahl der Methode ist die Frage, welche *Art von Ergebnis* benötigt wird. Wird beispielsweise eine tolerierbare Gefährdungsrate (THR) vorgegeben, muss zwangsläufig eine quantitative Analyse des Systems durchgeführt werden.

7.5.2 Geeignete Methoden zur Bewertung von Sicherheitsschichten

Für Sicherheitsschichten – als Teil sicherheitsrelevanter Systeme aus dem Bereich der Eisenbahn – sind die Anforderungen der CENELEC-Normen maßgebend. Hier sind insbesondere die vorgegebene Struktur und der Inhalt des Sicherheitsnachweises aus der DIN EN 50129 [DIN03] zu beachten. Der Sicherheitsnachweis wird für ein System geführt, das in der Regel mehr als eine Sicherheitsschicht umfasst. So ist zu unterscheiden zwischen Methoden zur *Bewertung einer einzelnen Sicherheitsschicht* und Methoden zur *Bewertung eines Systems* unter Berücksichtigung seiner Sicherheitsschichten. Idealerweise sollte eine Methode zur Bewertung einer einzelnen Sicherheitsschicht so gestaltet sein, dass ihre Ergebnisse für die Bewertung des Gesamtsystems weiterverwendet werden können.
Da der Begriff der Sicherheitsschicht in der vorliegenden Arbeit erst definiert wurde, existieren noch keine Methoden, die speziell auf die Bewertung von Sicherheitsschichten zugeschnitten sind. Eine solche Methode zu entwickeln, würde den Rahmen der vorliegenden Arbeit sprengen. Daher soll an dieser Stelle nur betrachtet werden, inwiefern bereits existierende Methoden für diese Aufgabe geeignet sind.

Um eine (quantitative) Bewertung der Sicherheit einer einzelnen SiS vorzunehmen, ist die FTA (Abschnitt 5.6) gut geeignet. Durch sie kann prinzipiell eine Gefährdungsrate für eine SiS berechnet werden, die in einer Gesamtsystem-FTA weiterverwendet werden kann. Hierbei wird durch die Funktion der SiS der funktionale Ansatz der CENELEC-Normen berücksichtigt. Schwierig wird die Berechnung einer Gefährdungsrate, wenn die Barriere der SiS neben technischen Komponenten auch menschliche oder organisatorische Faktoren enthält. Hier ist die Betrachtung entsprechender Ausfallraten noch ein aktuelles Forschungsthema. Allerdings liegt dieses Problem nicht in der Modellierung von Sicherheitsschichten begründet, denn durch die Modellierung werden dem System keine Teile hinzugefügt. Vielmehr handelt es sich um ein generelles Problem.

Ein weiterer Ansatz zur *quantitativen* Bewertung eines Systems und seiner Sicherheitsschichten ist der *energiebezogene Ansatz*. Bei einem energiebezogenen Ansatz wird das Risiko (als Kombination von Eintretenswahrscheinlichkeit und Schadensschwere) unter Zuhilfenahme der im System vorhandenen und ggf. freiwerdenden Energie bestimmt. Dieser Ansatz korrespondiert mit dem Konzept der Barriereanalyse, die Maßnahmen zum Schutz gegen Energie analysiert und die zusammen mit der FTA als Basis für die ISES-Methode verwendet wurde. Ein energiebezogener Ansatz bietet sich vor allem in Bereichen an, in denen große Energiemengen kontrolliert werden müssen, z. B. in der chemischen und der Prozessindustrie oder der Kernenergie, er wird aber auch im Eisenbahnbereich bei Weber [Web10] bereits diskutiert.

Bei einer rein *qualitativen* Betrachtung einzelner Sicherheitsschichten bietet sich – insbesondere im Hinblick auf den Austausch von SiS (siehe Abschnitt 7.6) – ein direkter *Vergleich* an. Dabei können verschiedene Aspekte der Sicherheitsschichten betrachtet werden, z. B. die Art der SiS, ob sie aktiviert werden muss oder deaktiviert werden kann, ob Menschen an der Funktion beteiligt sind, welche Schwächen die SiS haben, wie hoch ihre Kosten sind etc. Ziel einer solchen Betrachtung ist immer die Frage: Welche Sicherheitsschicht ist für den Anwendungsfall besser geeignet?

Wenn die vergleichende Betrachtung in *semi-quantitativer* Form erfolgen soll, kann z. B. ein Ansatz wie der der Risikoprioritätszahlen der Fehler-Möglichkeits-, Einfluss- und Kritikalitäts-Analyse (FMECA) (siehe z. B. [Bra05a]) gewählt werden.

Für eine Bewertung der Sicherheit eines Systems inklusive seiner Sicherheitsschichten ist prinzipiell jede Methode geeignet, die auch heute im Bereich der Eisenbahn zur Bewertung von Sicherheit oder Risiko eines Systems verwendet wird. Sollen die Erkenntnisse aus der Identifikation von Sicherheitsschichten dabei genutzt werden, so ist den Methoden der Vorrang zu geben, die das Konzept von Barrieren berücksichtigen, wie z. B. der ETA (Abschnitt 5.7). Ebenfalls gut geeignet ist die FTA. Die verschiedenen SiS eines Systems lassen sich aufgrund der Unabhängigkeitskriterien hier gut integrieren. Welche Methode man zur Sicherheitsbewertung des Systems auch verwendet, es empfiehlt sich in jedem Fall, eine CCF-Analyse durchzuführen, wie dies auch von der DIN EN 50129 [DIN03] gefordert wird.

7.6 Vorgehen zum Austausch von Sicherheitsschichten

Heutzutage kommt es in Europa immer seltener vor, dass Eisenbahnsysteme gänzlich neu „auf die grüne Wiese“ gebaut werden. Stattdessen werden immer häufiger Änderungen an bestehenden Eisenbahnsystemen vorgenommen. Die Gründe hierfür sind vielfältig: alte Bauteile werden abgekündigt und sind als Ersatzteile nicht mehr verfügbar, neue Technik wird auf den Markt gebracht, die europäische Harmonisierung erfordert das Umrüsten von Strecken und Fahrzeugen, die Sicherheit eines Systems soll verbessert werden oder es sollen Kosten gespart werden. Von einer Änderung eines Systems sind oft auch seine Sicherheitsschichten betroffen. Durch Änderungen an den Barrieren und / oder Funktionen des bestehenden Systems werden die Sicherheitsschichten, die diese Barrieren oder Funktionen enthalten, verändert oder ausgetauscht. Dadurch ändert sich in der Regel auch die Leistungsfähigkeit der Sicherheitsschicht, d. h. ihre Sicherheit.

Wichtige Anwendungen für das Modell der Sicherheitsschichten sind daher das Beurteilen von Veränderungen bestehender Systeme und das Bewerten von Alternativen – in Bezug auf die Sicherheit des Systems. Das Modell der Sicherheitsschichten kann hier bei der Entscheidungsfindung unterstützen, indem es die Unterschiede verdeutlicht.
Im Folgenden wird das Vorgehen für den Austausch einer Sicherheitsschicht (SiS) eines bestehenden Systems beschrieben (siehe auch Abbildung 7.7). Für die Beurteilung verschiedener Alternativen sowie für den Austausch mehrerer Sicherheitsschichten ist das Vorgehen entsprechend.

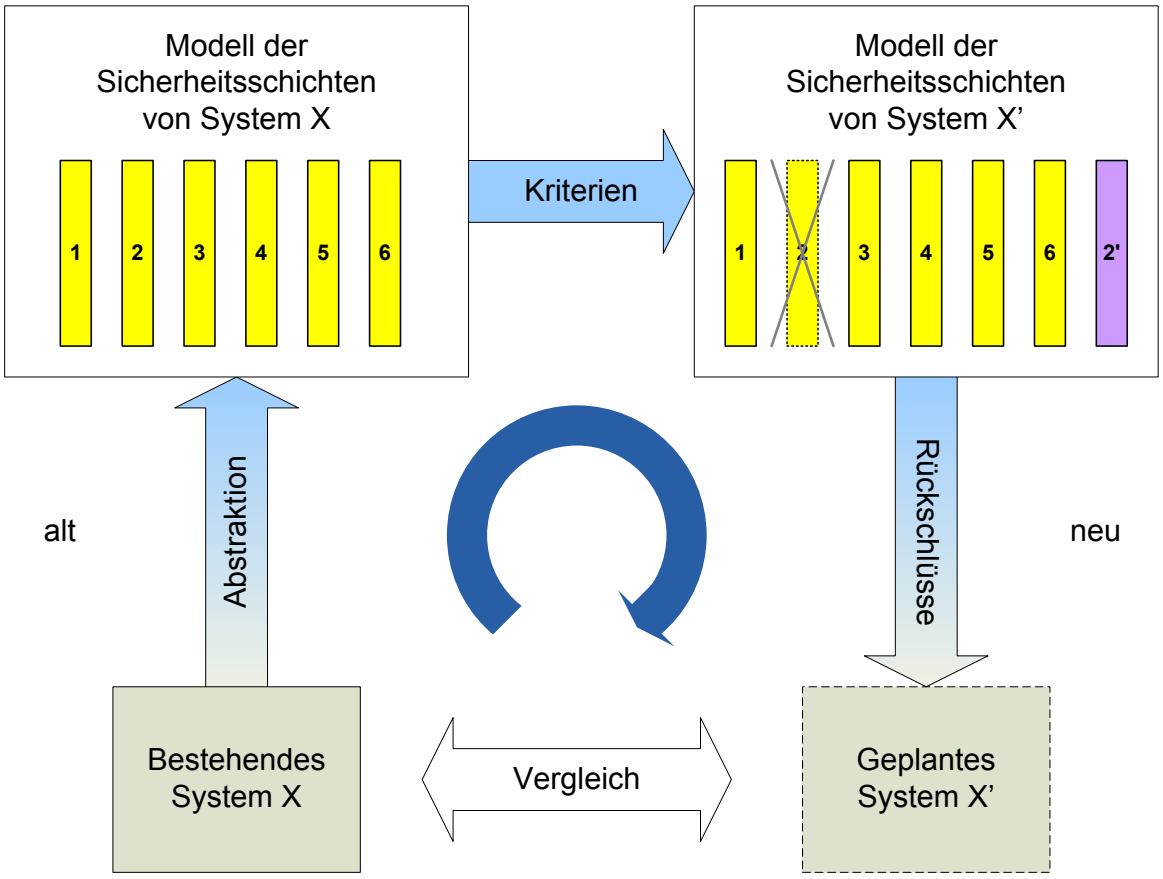

Abbildung 7.7: Vorgehen zum Austausch von Sicherheitsschichten

Zunächst muss die ISES-Methode auf das bestehende System angewendet werden, um ein Modell der Sicherheitsschichten dieses Systems zu erhalten. Anschließend wird die Sicherheitsschicht identifiziert, die ausgetauscht werden soll. Eine Veränderung einer Sicherheitsschicht entspricht dem Austausch dieser Sicherheitsschicht gegen eine andere, veränderte Sicherheitsschicht. Die Identifikation der betroffenen Sicherheitsschicht kann z. B. anhand ihrer *Barriere* erfolgen – häufig werden Änderungen an bestehenden Systemen durch den Einsatz neuer Technik beschrieben. Im einfachsten Fall wird nur die Barriere der Sicherheitsschicht ausgetauscht – gegen eine Barriere, die vorher im System noch nicht enthalten war – und die Funktion bleibt dieselbe. In diesem Fall genügt es, für die neue SiS eine Prüfung der Kriterien aus Abschnitt 3.2 durchzuführen. Besondere Vorsicht hingegen ist geboten, wenn die Barriere der neuen SiS nicht neu hinzugefügt wird, sondern ein bereits zuvor vorhandenes Systemelement dafür genutzt wird. Dann müssen zusätzlich die Unabhängigkeitskriterien aller vorhandenen Sicherheitsschichten des Systems neu geprüft werden. Entsprechendes gilt, wenn eine Funktion verändert wird, die Teil einer SiS ist. Auch hierdurch wird eine SiS verändert bzw. ausgetauscht, und die Kriterien für Sicherheitsschichten müssen neu geprüft werden.
Auf diese Weise entsteht ein Modell der Sicherheitsschichten des neuen, geänderten Systems noch während der Planungsphase, also bevor die Änderung umgesetzt wird. Durch den Austausch einer Sicherheitsschicht ändert sich in der Regel ihre Sicherheit. Diese zu verändern ist häufig sogar

das Ziel der Systemänderung. Durch das Modell der Sicherheitsschichten werden die Änderungen bzgl. der Sicherheit deutlich gemacht und so kann ein Vergleich zwischen dem bestehenden und dem veränderten System stattfinden. Es kann beurteilt werden, ob sich die Sicherheit des Systems durch die Änderung möglicherweise verschlechtert, und ob zusätzliche Maßnahmen ergriffen werden müssen, um das wieder auszugleichen. Die Bewertung des veränderten Systems erfolgt dabei so wie die Bewertung des bestehenden Systems (siehe Abschnitt 7.5).
Das Modell der Sicherheitsschichten erleichtert so die Entscheidungsfindung und auch die Bewertung der Auswirkungen auf die Sicherheit. Insbesondere für Begutachtung und Zulassung ergeben sich hier Vorteile, da die Änderung mit Bezug auf die Sicherheit klar beschrieben wird. Durch die Unabhängigkeitsanforderungen, die an Sicherheitsschichten gestellt werden, erfolgt der Austausch von Sicherheitsschichten relativ rückwirkungsarm. Da jedoch die Sicherheitsschichten nur einen Teil des Systems modellieren und von technischen Veränderungen nicht nur die Existenz von Sicherheitsschichten betroffen ist, sondern sich auch die Löcher in den Sicherheitsschichten verändern können, kann auf eine CCF-Analyse beim Austausch von Sicherheitsschichten nicht verzichtet werden.

8 Anwendungsbeispiel: Bahnübergang

Die Anwendung der ISES-Methode aus Kapitel 6 soll an einem Beispiel demonstriert werden. In diesem Kapitel wird dieses Anwendungsbeispiel vorgestellt.
Ein klassisches Anwendungsbeispiel für Modellierungsfragen im Bereich der Eisenbahn ist das des funkbasierten Bahnübergangs aus dem FunkFahrBetrieb (FFB). Dieses Beispiel wurde im Schwerpunktprogramm „Softwarespezifikation“ der Deutschen Forschungsgemeinschaft und auch auf der Konferenz *Forms 2000* als Referenzfallstudie genutzt [Jan00]. Auf der *Forms 2000* wurden vier Beiträge vorgestellt, die den FFB-Bahnübergang als Anwendungsbeispiel verwenden, um u. a. verschiedenen Modellierungen vergleichen zu können, siehe [Sch00]. Der FFB-Bahnübergang ist ein räumlich und funktional gut abgrenzbares Beispiel mit relativ geringer (aber nicht zu geringer) Komplexität. Derartige Anwendungsbeispiele haben den Vorteil, dass sich Modellierungsexperten aus verschiedenen Domänen leicht einarbeiten können. Bei hoch komplexen Anwendungsbeispielen bliebe die Modellierung den Domänenexperten vorbehalten. Ein weiterer Vorteil von kleinen, übersichtlichen und relativ einfachen Beispielen ist, dass sie leicht zu verstehen sind. Der Leser braucht kein Experte in diesem System zu sein und kann sich ganz auf den Kern des Beitrags konzentrieren: die Modellierung bzw. die Anwendung einer bestimmten Methode.
Den FFB-Bahnübergang als Anwendungsbeispiel für die ISES-Methode zu verwenden, würde einen Vergleich der Modellierung von Sicherheitsschichten mit den Modellen von der *Forms 2000* ermöglichen und hätte zugleich die oben beschriebenen Vorteile. Allerdings ist der funkbasierte Bahnübergang aus [Jan00] Teil des DB-Projekts FunkFahrBetrieb, das nur als Pilotprojekt realisiert wurde. Der FFB-Bahnübergang gehört somit nicht zu den heute üblicherweise verwendeten Bahnübergängen. Aus diesem Grund wird der FFB-Bahnübergang von vielen Praktikern als theoretisch-akademisches Beispiel angesehen. Darunter leidet bisweilen auch die Akzeptanz von Beiträgen, die den FFB-Bahnübergang als Anwendungsbeispiel verwenden.
Ein Ziel der vorliegenden Arbeit ist es, einen Grundstein für die Anwendung der ISES-Methode zu legen. Ein Anwendungsbeispiel, das im Betrieb eingesetzt wird, ist dafür von großem Nutzen. Es soll daher ein anderes Beispiel als der FFB-Bahnübergang verwendet werden, eines, das für die Praxis relevanter ist. Dennoch sollen die Vorteile des Anwendungsbeispiels FFB-Bahnübergang, die leichte Verständlichkeit, die räumliche und funktionale Abgrenzbarkeit und die geringe Komplexität auch für das hier verwendete Beispiel genutzt werden. Zusätzlich ist zumindest eine gewisse Vergleichbarkeit mit den Ergebnissen von der *Forms 2000* wünschenswert. Daher soll als Anwendungsbeispiel für die ISES-Methode ebenfalls ein Bahnübergang verwendet werden. Dieser Bahnübergang soll jedoch ein in der Praxis verwendeter Typ Bahnübergang sein. Welcher Typ, wird im folgenden Abschnitt diskutiert.
Neben der Relevanz für die bahnbetriebliche Praxis und den anderen, oben genannten Vorteilen, haben Bahnübergänge noch einige weitere Eigenschaften, die sie zu guten Anwendungsbeispielen machen: Sie sind in Deutschland überall zahlreich vorhanden und aufgrund ihrer Funktion für Straßenverkehrsteilnehmer meist frei zugänglich (im Gegensatz zu einem Stellwerk beispielsweise). Dadurch erhöhen sich die Verständlichkeit und die Greifbarkeit des Beispiels. Durch die Schnittstelle zur Straßenseite kann darüber hinaus geprüft werden, ob die ISES-Methode auch domänenübergreifend zum Einsatz kommen kann.
Ein weiteres Argument für die Wahl eines Bahnübergangs als Anwendungsbeispiel ist seine Relevanz für das Thema Sicherheit. An Bahnübergängen geschehen jedes Jahr zahlreiche Unfälle mit Toten [BM08]. Sie sind Unfallschwerpunkte, sowohl für den Schienen- als auch für den Straßenver-

kehr [Sch07]. Daher sind Bahnübergänge für Sicherheitsbetrachtungen ein ausgesprochen relevantes Thema.

8.1 Arten von Bahnübergängen

Es gibt zwei grundsätzliche Arten, Bahnübergänge zu klassifizieren: aus Sicht des Straßenverkehrs und aus Sicht des Bahnverkehrs. Aus Sicht des Straßenverkehrs sind vor allem die Art der Warnung vor dem herannahenden Zug und bei Bedarf aktivierte Barrieren, die den Straßenverkehrsteilnehmern den Weg versperren, relevant: Andreaskreuze, Lichtzeichen und Schranken. Die Europäische Eisenbahnagentur (ERA) unterscheidet folgende Klassen von Bahnübergängen [LKEK+08]:

A Aktiver Bahnübergang

- A.1 Automatischer Schutz / Warnung
  - A.1.1 Straßenseitiger Schutz (Schranken / Tore)
  - A.1.2 Straßenseitige Warnung (sichtbar / hörbar / physisch)
  - A.1.3 Straßenseitiger Schutz und Warnung
- A.2 Manueller Schutz / Warnung
  - A.2.1 Straßenseitiger Schutz (Schranken / Tore)
  - A.2.2 Straßenseitige Warnung (sichtbar / hörbar / physisch)
  - A.2.3 Straßenseitiger Schutz und Warnung

B Passiver Bahnübergang

Aus Sicht des Eisenbahnverkehrs ist vor allem relevant, wie die Bahnübergangssicherung angestoßen wird, ob und wie geprüft wird, ob der Bahnübergang ordnungsgemäß gesichert wurde und wie diese Information wohin weiter geleitet wird. Daher konzentriert sich die Betrachtung auf die Signale und die Überwachungsart des Bahnübergangs.

Wie Bahnübergänge in Deutschland gesichert werden müssen, wird in der EBO [Bun12], § 11 geregelt. Tabelle 8.1 gibt einen Überblick über die in Deutschland verwendeten Bahnübergangs-Typen, ihre Überwachungs- und Sicherungsarten. Die Funktions-Prinzipien der Bahnübergangs-Typen in Tabelle 8.1 wurden zum Teil [Hen02] entnommen.

Von den in Tabelle 8.1 aufgeführten Überwachungsarten von Bahnübergängen ist die Überwachungsart ÜS als Anwendungsbeispiel am besten geeignet. Ein Bahnübergang mit dieser Überwachungsart ist ausreichend komplex, jedoch nicht zu komplex. Der ÜS-Bahnübergang ist technisch gesichert. Er kann räumlich gut abgegrenzt werden, da seine Einschaltung automatisch zugbewirkt und damit autark vor Ort erfolgt. Da die Einschaltung automatisch erfolgt, werden menschliche Einflüsse bei der Betrachtung reduziert. Menschliche Einflüsse können bei der Analyse sehr komplex sein und sind stets eine Herausforderung für Modellierung und Methoden. Auch am ÜS-Bahnübergang gibt es menschliche Einflüsse, z. B. durch Triebfahrzeugführer und Straßenverkehrsteilnehmer. Bahnübergänge mit der Überwachungsart ÜS kommen in Deutschland häufig vor, sie werden als Bahnübergang auf öffentlichen Straßen mit Kraftverkehr, z. B. in Städten eingesetzt. Der ÜS-Bahnübergang hat zudem Ähnlichkeit mit dem FFB-Bahnübergang. Allerdings wird der Einschaltbefehl nicht per Funk vom Zug, sondern von einem streckenseitigen Einschaltkontakt an den Bahnübergang übermittelt. Zudem arbeitet die Fahrzeugsteuerung auf dem Zug anders als in der Referenzfallstudie FFB-Bahnübergang. Aus den aufgeführten Gründen soll zur Demonstration der ISES-Methode ein ÜS-Bahnübergang verwendet werden.

Tabelle 8.1: Bahnübergangs-Typen in Deutschland sowie Auswahl eines Beispiel-Bahnübergangs

Überwachungs-art / BÜ-Typ	**Charakteristik**	**Prinzip**, z.T. nach [Hen02]	**Sicherungsart**	**Einschaltart**
ÜS	Überwachungssignal, überwacht durch Tf	stellen - fahren - prüfen	technisch	zuggesteuert
$ÜS_{OE}$	Überwachungssignal mit optimierter Einschaltung, überwacht durch Tf, ÜS liegt vor dem Einschaltpunkt, kontrolliert nur Einschaltbereitschaft	prüfen – fahren – stellen	technisch	zuggesteuert
Hp	hauptsignalüberwacht, durch Hauptsignal gedeckt	stellen – prüfen – fahren	technisch	fahrstraßenbewirkt
Hp_{OE}	Hauptsignalabhängigkeit mit optimierter Einschaltung, Verschmelzung der Überwachungsarten Hp und Fü, hauptsignalüberwacht	prüfen - fahren - stellen	technisch	zuggesteuert
Fü	fernüberwacht durch Fdl, kein Signal für Tf, keine Signalabhängigkeit zur Stellwerksanlage, signaltechnisch sichere Ansteuerung	fahren – stellen – prüfen	technisch	zuggesteuert
Anrufschranke	in Grundstellung geschlossen, nur bei Anruf geöffnet, bedienerüberwacht	geschlossen lassen	technisch	bedienergesteuert
handgesteuerte Anlagen	aktiviert und überwacht durch Tf	halten – stellen – prüfen – fahren	technisch	bedienergesteuert
Ü	Übersicht, keine Überwachung	gesehen werden	nicht-technisch	keine
Ü + P	Übersicht und Pfeifen, keine Überwachung	gesehen werden, warnen	nicht-technisch	keine
P + Lf	Pfeifen und Geschwindigkeitsbeschränkung auf 20 km/h oder 60 km/h je nach Wegeart, zum Erreichen der Übersicht, keine Überwachung	gesehen werden, warnen	nicht-technisch	keine
Postensicherung	Posten hält den Straßenverkehr an, keine Überwachung	sichern - fahren	nicht-technisch	keine

8.2 Beschreibung eines Bahnübergangs mit Überwachungssignal

Als Anwendungsbeispiel wird der folgende in Deutschland verwendete Typ Bahnübergang dienen: ein Bahnübergang mit Halbschranken (HS) und ÜS wie in Abbildung 8.1 dargestellt. Bahnübergänge mit der Überwachungsart ÜS werden mit Hilfe eines Einschaltkontakts im Gleis zuggesteuert eingeschaltet, sobald sich ein Zug dem Bahnübergang nähert. Dort, wo der Einschaltkontakt liegt, steht eine Rautentafel (Signal Bü 2). Sie kündigt ein Überwachungssignal an und markiert zugleich den Anfang der Einschaltstrecke. Das Überwachungssignal gibt dem Triebfahrzeugführer Rückmeldung darüber, ob der Bahnübergang tatsächlich eingeschaltet wurde. Wenn die Einschaltung des Bahnübergang ordnungsgemäß erfolgt ist, beginnt das Überwachungssignal weiß zu blinken. Damit wird dem Triebfahrzeugführer das Signal Bü 1 gegeben: „Der Bahnübergang darf befahren werden“ [Deu08]. Nachdem der Zug den Ausschaltkontakt passiert hat, wird die Bahnübergangssicherung ausgeschaltet und der Bahnübergang wird wieder für den Straßenverkehr freigegeben.

Sollte der Bahnübergang gestört sein und nicht eingeschaltet werden können, bleibt das Überwachungssignal dunkel. In diesem Zustand zeigt das Überwachungssignal das Signal Bü 0: „Halt vor dem Bahnübergang! Weiterfahrt nach Sicherung“ [Deu08]. Der 1000-Hz-Magnet der punktförmigen Zugbeeinflussung (PZB), der am Überwachungssignal liegt, ist dann wirksam. Nachdem der Zug das Signal mit dem 1000-Hz-Magneten passiert hat, muss der Triebfahrzeugführer durch Drücken der Wachsamkeitstaste quittieren, dass er das Signal wahrgenommen hat – sonst wird er von der PZB zwangsgebremst. Anschließend muss er gemäß der Richtlinie 408 der Deutschen Bahn AG [Deu06], Modul 0671, seinen Zug vor dem Bahnübergang zum Stehen bringen und den Bahnübergang manuell sichern.

Bahnübergänge der Überwachungsart ÜS arbeiten autark. Das bedeutet, es ist kein Personal vor Ort. Der zuständige Fahrdienstleiter, der seinen Arbeitsplatz im Stellwerk oder in einer Betriebszentrale hat, kann keinen direkten Einfluss auf den Bahnübergang nehmen. Im Fall einer Störung ist der Triebfahrzeugführer der einzige, der den Bahnübergang sichern und die Störung melden kann.

Aus Gründen der Übersichtlichkeit wird als Anwendungsbeispiel ein Bahnübergang mit nur einem Gleis verwendet. Eingleisige Strecken werden in der Regel in beiden Richtungen befahren. Entsprechend ist die Bahnübergangs-Technik im und am Gleis doppelt vorhanden – ein Mal für jede Richtung. Der Einfachheit halber soll im Beispiel jedoch nur eine Fahrtrichtung betrachtet werden.

Insgesamt gehören zum betrachteten Bahnübergangssystem:

- ein Gleis
- eine Rautentafel
- ein Überwachungssignal mit einem 1000-Hz-Magneten der PZB
- ein Einschaltkontakt
- ein Ausschaltkontakt
- Halbschranken
- Lichtzeichen für den Straßenverkehr

Ebenfalls betrachtet werden:

- ein Zug mit fahrzeugseitiger PZB-Einrichtung
- der Triebfahrzeugführer

Andreaskreuze, Baken und Straßenfahrzeuge (PKW, LKW, ...) gehören ebenfalls zum Bahnübergangssystem, werden für die Demonstration der Methode aber nicht benötigt und daher nicht weiter betrachtet.

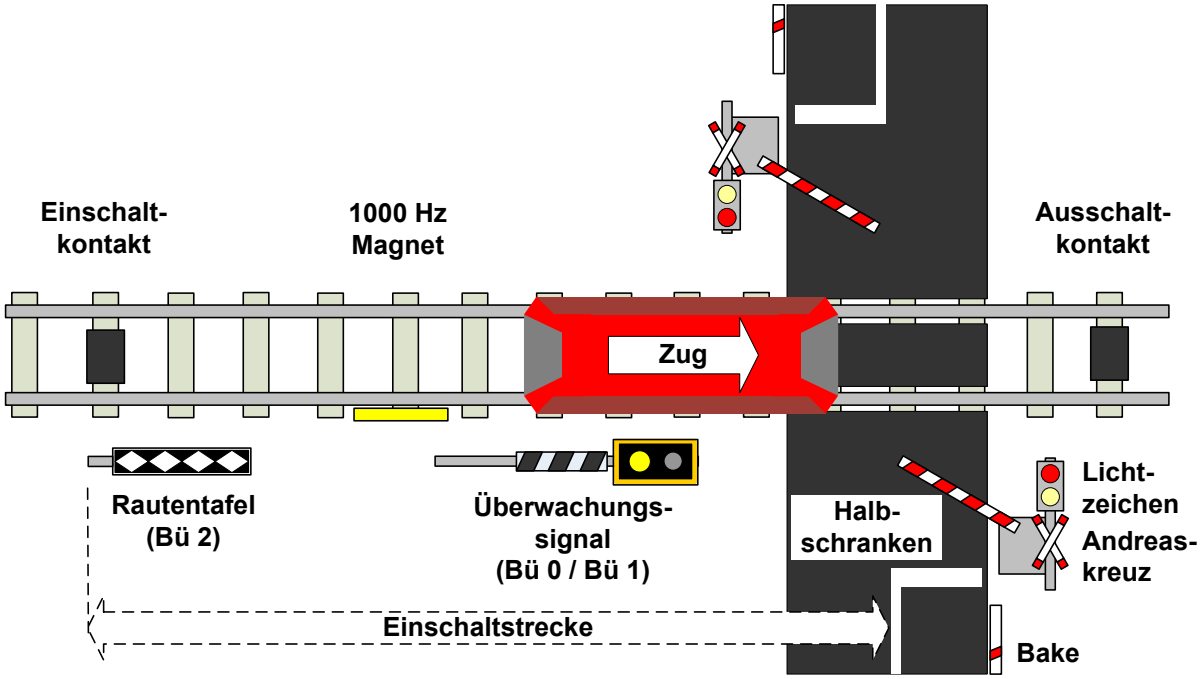

Abbildung 8.1: Bahnübergang mit Überwachungssignal

8.3 Zu untersuchende Gefährdung

Um die ISES-Methode anwenden zu können, muss zunächst die zu betrachtende Gefährdung festgelegt werden. Fragt man einen Menschen nach einer Gefährdung, die untersucht werden soll, so ist die Wahrscheinlichkeit groß, dass er einen Unfall statt einer Gefährdung benennt. Diese beiden Begriffe werden im Sprachgebrauch oft vermischt und stellenweise sogar synonym verwendet. Der kleine, aber bedeutsame Unterschied zwischen Gefährdung und Unfall ist, dass eine Gefährdung eine Bedingung ist, die möglicherweise zu einem Unfall führen kann. Mit der ISES-Methode werden Systeme mit Hinblick auf Gefährdungen, nicht mit Hinblick auf Unfälle untersucht. Der Grund dafür ist einfach: Die Erkenntnisse aus der Analyse sollen zur Verfügung stehen, bevor es zu einem Unfall kommt. Indem man Gefährdungen analysiert, analysiert man zugleich eine ganze Gruppe ähnlicher möglicher Unfälle.

Um die relevanten Gefährdungen für das zu untersuchende System zu identifizieren, kann man bereits vorhandene Gefährdungslisten nutzen. Ein anderer Weg ist, von möglichen Unfallarten auszugehen und die Bedingungen / die Gefährdungen, die zu diesen Unfällen führen können, zu identifizieren. Für das Beispiel des Bahnübergangs soll der Weg über Unfallarten gegangen werden.

In der Richtlinie über die Eisenbahnsicherheit [Eur04] wird gefordert, dass die Sicherheitsbehörden der ERA jährlich über bestimmte sogenannte „gemeinsame Sicherheitsindikatoren“ Bericht erstatten. Einige dieser Sicherheitsindikatoren sind unfallbezogen. Für die Berichterstattung wird zwischen folgenden Unfallarten unterschieden:

- Kollisionen von Zügen einschließlich Kollisionen mit Hindernissen innerhalb des Lichtraumprofils
- Zugentgleisungen
- Unfälle auf Bahnübergängen einschließlich solcher, an denen Fußgänger beteiligt sind
- Unfälle mit Personenschäden, die von in Bewegung befindlichen Eisenbahnfahrzeugen verursacht wurden, mit Ausnahme von Suiziden
- Suizide
- Fahrzeugbrände
- Sonstige Unfälle

Auf einem Bahnübergang können prinzipiell alle diese Unfallarten geschehen. Es kann auf einem Bahnübergang z. B. zu einer Entgleisung oder einem Brand kommen. Eine bestimmte Unfallart ist jedoch an einem Bahnübergang besonders relevant: Ein Unfall auf einem Bahnübergang in Form eines Zusammenpralls zwischen einem Zug und einem Straßenverkehrsteilnehmer (PKW, LKW, Fahrradfahrer, Fußgänger, . . .). Für diese Art Unfall besteht am Bahnübergang ein besonders hohes Risiko, weil dort Straßenverkehrsteilnehmer und Züge den gleichen Raum benutzen, und zwar regelmäßig. Bei den anderen Unfallarten (mit Ausnahme evtl. des Aufpralls auf ein Hindernis), bietet der Bahnübergang keine bessere „Gelegenheit“ als andere Teile der Eisenbahnstrecke. Daher macht es Sinn, am Bahnübergang eine Gefährdung zu untersuchen, die zu diesem Unfall führen kann. Eine solche Gefährdung, die zu einem Zusammenprall zwischen einem Zug und einem Straßenfahrzeug führen kann, ist: „Zug befährt ungesicherten Bahnübergang“. Es gibt noch weitere Gefährdungen, die zu einem Zusammenprall zwischen einem Zug und einem Straßenverkehrsteilnehmer führen können, z. B. einen Autofahrer, der die geschlossenen Halbschranken umfährt, um noch schnell vor dem Eintreffen des Zuges auf die andere Seite zu kommen. Hierbei handelt es sich jedoch um ein eindeutiges Fehlverhalten des Straßenverkehrsteilnehmers. Aus Sicht der Eisenbahn ist die Gefährdung „Zug befährt ungesicherten Bahnübergang“ diejenige, die zweifellos in ihren Zuständigkeitsbereich fällt. Daher soll für das Beispiel des Bahnübergangs diese Gefährdung untersucht werden.

Anmerkung: Das Wort „ungesichert“ wird hier bei der Bezeichnung der Gefährdung verwendet, um zu beschreiben, dass die Bahnübergangssicherung (sowohl die technische als auch die nichttechnische) ihre Funktion nicht ausreichend erfüllt. Demgegenüber steht die zweite, ebenfalls gebräuchliche Bedeutung des Begriffs „gesichert“ bei der Beschreibung von Bahnübergängen: Ein Bahnübergang ist entweder „technisch gesichert“ oder „nichttechnisch gesichert“, d. h. er verfügt entweder über technische Bahnübergangssicherungsanlagen wie z. B. Lichtzeichen und Schranken oder die Sicherung erfolgt nichttechnisch, z. B durch Übersicht (siehe Tabelle 8.1). Einen ungesicherten Bahnübergang gibt es in diesem Kontext nicht. Trotz dieser unterschiedlichen Verwendung des Worts „gesichert“, ist die Bezeichnung „ungesicherter Bahnübergang“ eindeutig und allgemein verständlich und wird daher im Folgenden verwendet.

9 Anwendung der ISES-Methode auf den Beispiel-Bahnübergang

Im Folgenden wird die in Kapitel 6 vorgestellte ISES-Methode mit ihren Schritten A bis D auf das in Kapitel 8 vorgestellte Beispiel eines Bahnübergangs mit Halbschranken und Überwachungssignal angewendet. Nach der Identifikation der Sicherheitsschichten des Bahnübergangs in Schritt D der ISES-Methode wird dieses Beispiel genutzt, um das in Abschnitt 7.6 beschriebene Vorgehen zum Austausch von Sicherheitsschichten zu verdeutlichen. Dies geschieht durch die Veränderung des Beispiel-Bahnübergangs durch die Einführung des *European Train Control System (ETCS)*.

9.1 Schritt A: Fehlerbaumanalyse

9.1.1 Durchführung

Im Schritt A werden eine Systembeschreibung, eine zu betrachtenden Gefährdung und ein zugehöriger Fehlerbaum erstellt oder zusammengetragen. Die Systembeschreibung kann Abschnitt 8.2 entnommen werden. Die zu betrachtende Gefährdung ist „Zug befährt ungesicherten Bahnübergang“ (siehe Abschnitt 8.3). Für diese Gefährdung wird ein *qualitativer Fehlerbaum* benötigt.

Im Rahmen dieses Beispiels soll es genügen, nur den Teil des Systems zu betrachten, der von der Eisenbahn beeinflussbar ist. Der Straßenverkehr wird nur insoweit betrachtet, wie es unbedingt notwendig ist. Dieses Vorgehen dient zum einen der Reduzierung der Komplexität des Beispiels. Zum anderen wird eine derartige Analyse in der Praxis von Personen durchgeführt, die eine klare Zielvorgabe (z. B. Zulassung der Bahnübergangssicherungsanlage) oder einen eingeschränkten Handlungsspielraum besitzen. Ein Hersteller einer Bahnübergangssicherungsanlage z. B. kann zwar in Abstimmung mit seinem Kunden die Bahnübergangssicherungsanlage verändern, aber nicht den Verlauf der Straße oder das Verhalten der Autofahrer.

Wie in Abschnitt 6.3 beschrieben, kann auf bereits existierende Fehlerbäume zurückgegriffen werden, sofern diese geeignet sind. Für die Gefährdung „Zug befährt ungesicherten Bahnübergang“ an einem Bahnübergang mit Überwachungssignal wurde bereits ein Fehlerbaum in [Sch10] veröffentlicht (siehe Abbildung A.1 in Anhang A). Dieser Fehlerbaum wäre prinzipiell geeignet, um im Rahmen der ISES-Methode verwendet zu werden. Allerdings ist der Fehlerbaum aus Abbildung A.1 ein aus Herstellersicht eher untypischer Fehlerbaum. Er enthält menschliche und auch betriebliche Aspekte. Auf diese Aspekte hat ein Hersteller nur sehr eingeschränkten Einfluss und sie unterliegen auch nicht seiner direkten Verantwortung. Daher beschränkt sich ein Hersteller bei der Erstellung von Fehlerbäumen in der Regel auf das technische System, das er liefert. Für die Demonstration der ISES-Methode soll ein herstellertypischer Fehlerbaum als Basis verwendet werden – ein Fehlerbaum wie er auch im Rahmen der üblichen Sicherheitsnachweisführung erstellt werden könnte. Ein solcher Fehlerbaum ist in Abbildung 9.1 dargestellt.

Dieser Fehlerbaum ist für die Analyse mit der ISES-Methode geeignet, da sein Top-Ereignis der zu untersuchenden Gefährdung entspricht. Der Fehlerbaum besitzt eine geeignete Detaillierungstiefe: Er besitzt unterhalb des Top-Ereignisses vier Ebenen, enthält ODER-Verknüpfungen, jedoch keine Ereignis-Dopplungen und ist nicht vermascht.

9.1.2 Ergebnis

Zu den Ergebnissen dieses Schritts gehören die Beschreibung des analysierten Systems inklusive seiner Systemgrenzen (siehe Abschnitt 8.2) und die Festlegung der zu betrachtenden Gefährdung: „Zug befährt ungesicherten Bahnübergang“. Das wichtigste Ergebnis dieses Schritts ist der qualitative Fehlerbaum für die betrachtete Gefährdung des zu untersuchenden Systems (siehe Abbildung 9.1[1]). Er wird in Schritt B weiter analysiert.

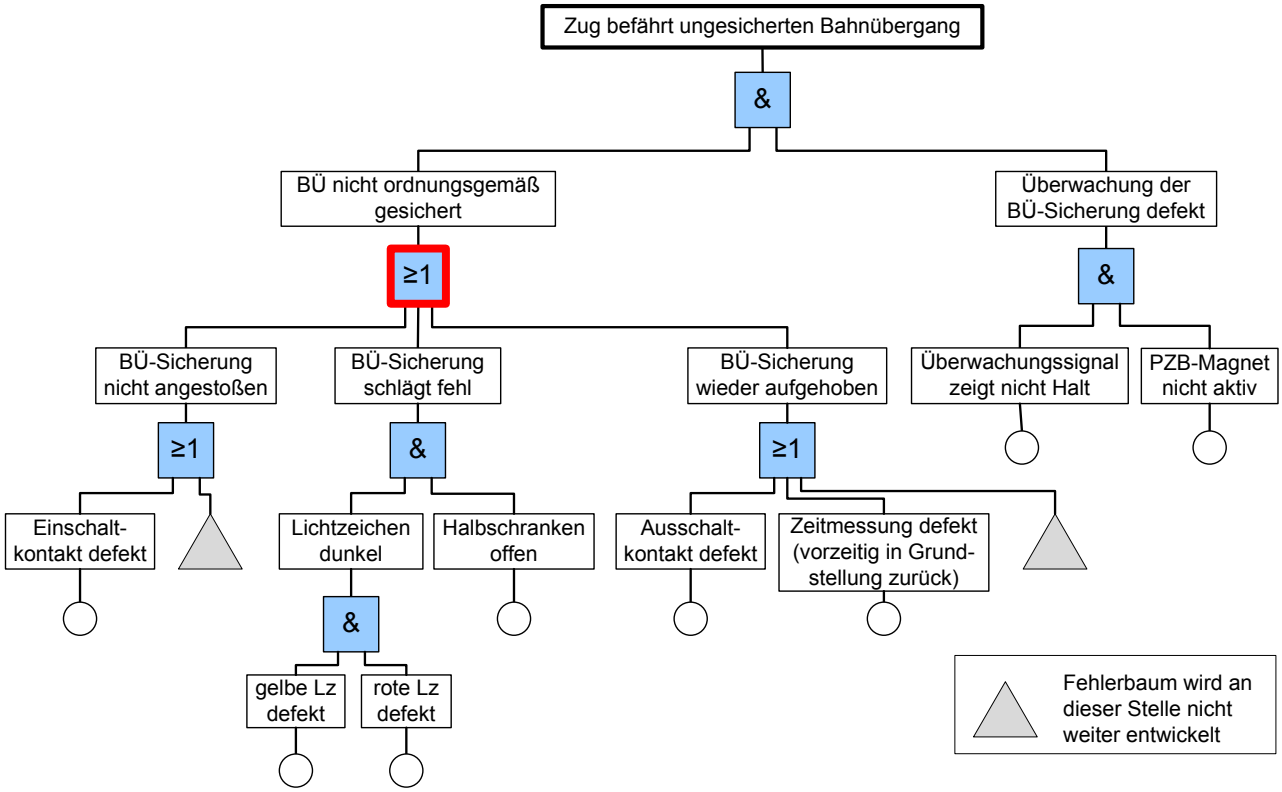

Abbildung 9.1: Fehlerbaum aus Sicht eines Herstellers für einen Bahnübergang mit Überwachungssignal

9.2 Schritt B: Identifikation von Barrieren mit Hilfe der Fehlerbaumanalyse

9.2.1 Durchführung

In Schritt B werden mit Hilfe des Fehlerbaums aus Abbildung 9.1 die Barrieren identifiziert, die im Beispiel-System des Bahnübergangs mit Überwachungssignal vorhandenen sind. Dazu werden vom Top-Ereignis, der Wurzel des Fehlerbaums, aus die ersten auftretenden ODER-Verknüpfungen gesucht. Der Fehlerbaum aus Abbildung 9.1 enthält genau eine solche erste ODER-Verknüpfung. Sie ist in Abbildung 9.1 durch einen roten Rahmen markiert. Die Elemente direkt oberhalb und unterhalb dieser ersten ODER-Verknüpfung sind ein Ansatzpunkt für die Suche nach den vorhandenen Barrieren. Unterhalb der rot umrandeten ODER-Verknüpfung findet sich der Fall 2, „Aktivierung – Funktion – Deaktivierung“, aus Abschnitt 6.4.3. Das Ereignis „BÜ nicht ordnungsgemäß gesichert“ kann dadurch verursacht werden, dass die Bahnübergangssicherung nicht angestoßen wird

[1] Abbildung 9.1 enthält bereits eine rot markierte ODER-Verknüpfung als Vorgriff auf das Ergebnis von Schritt B.

(Aktivierung), fehl schlägt (Durchführung) oder wieder aufgehoben wird (Deaktivierung). Die gesuchte Barriere befindet sich unter der ODER-Verknüpfung, sie wird in allen drei Elementen darunter genannt: Bahnübergangssicherung bzw. die Bahnübergangssicherungsanlage. Unter diesen drei Elementen befinden sich im mittleren Zweig weitere UND-Verknüpfungen. Daher kann die Barriere Bahnübergangssicherung mit Hilfe des Fehlerbaums weiter unterteilt werden – bis zu einer weiteren ODER-Verknüpfung oder, wie hier, bis zum Ende des Baums. Die resultierenden drei hintereinander liegenden Teilbarrieren sind: gelbe Lichtzeichen (Lz), rote Lz und Halbschranken.
Ein Beispiel für den Fall 1, die „Komponenten-Reihenschaltung“ aus Abschnitt 6.4.3, findet sich im Fehlerbaum aus Abbildung 9.1 nicht.
Im rechten Zweig des Fehlerbaums aus Abbildung 9.1 befindet sich keine ODER-Verknüpfung. Daher sind alle Blätter in diesem Zweig des Fehlerbaums Ansatzpunkte für vorhandene Barrieren. Da alle Blätter dieses Zweigs bis zum Top-Ereignis des Baums ausschließlich UND-verknüpft sind, beinhaltet jedes Blatt eine Barriere. Die Barrieren sind das Überwachungssignal und der PZB-Magnet.

9.2.2 Ergebnis

Die Ergebnisse dieses Schritts sind:

- Ein Fehlerbaum für die betrachtete Gefährdung des Bahnübergangs, in dem alle ersten auftretenden ODER-Verknüpfungen markiert sind: siehe Abbildung 9.1
- Eine Liste mit identifizierten Barrieren für diese Gefährdung:
  - gelbe Lichtzeichen
  - rote Lichtzeichen
  - Halbschranken
  - Überwachungssignal
  - PZB-Magnet

Jede der identifizierten Barrieren hat das Potenzial, das Eintreten des Top-Ereignisses zu verhindern. Die ersten drei Barrieren wirken dabei dem Zustand „ungesicherter Bahnübergang“ entgegen. Die anderen Barrieren können verhindern, dass der Zug diesen ungesicherten Bahnübergang befährt.
Anmerkung: Es wurde im Fehlerbaum davon ausgegangen, dass die PZB und das Überwachungssignal voneinander unabhängig sind. Das bedeutet, dass ein Fehler im Signal (Signal zeigt nicht Halt) keinen Einfluss auf den PZB-Magneten hat, also nicht dazu führt, dass der PZB-Magnet ebenfalls nicht aktiv ist. Vielmehr wurde davon ausgegangen, dass der PZB-Magnet aktiv sein kann, auch wenn das Signal versagt. Wäre der PZB-Magnet hingegen von der Stellung des Signals abhängig und würde das Signalbild abgreifen, um seine Funktion zu erfüllen (signalabhängig), dann würde es sich hier nicht um zwei unabhängige Barrieren handeln Die PZB würde dann die Qualität der Sicherheitsschicht verbessern, die das Überwachungssignal als Barriere enthält, könnte aber eigenständig keinen Unfall verhindern. Sie wäre ein „Lochstopfer“.

9.3 Schritt C: Identifikation von Barriere-Funktions-Paaren mit Hilfe von Checklisten

9.3.1 Durchführung

In Schritt C werden die Barrieren aus Schritt B ergänzt und vervollständigt. Mit Hilfe einer Checkliste werden den identifizierten Barrieren Funktionen zugeordnet und weitere Barrieren identifiziert. Für diese Arbeit werden als vorbereitende Maßnahme zunächst bereits vorhandene Checklisten zusammengetragen, ergänzt und auf das System angepasst. Im Anschluss an die Arbeit mit den Checklisten fließen die Erkenntnisse aus der Analyse in eine überarbeitetet Version der Checkliste ein, um sie für die nächste Analyse nutzbar zu machen.

C1: Vorbereitung der Checklisten

Die Basis-Checkliste aus Abschnitt 6.5, Tabelle 6.1, ist bis jetzt noch recht allgemein. Sie gilt für das gesamte Eisenbahnsystem und ist nicht bahnübergangsspezifisch. Bevor ein Modell der Sicherheitsschichten für einen bestimmten Teil des Bahnsystems aufgestellt wird, empfiehlt es sich als vorbereitende Maßnahme, die Checklisten auf Vollständigkeit zu überprüfen, gegebenenfalls anzupassen und um systemspezifische Aspekte zu ergänzen / zu erweitern. Hierzu werden Erkenntnisse aus anderen Quellen, z. B. aus anderen Projekten oder Vorschriften für die Gestaltung des Systems zusammengetragen.
Um die Checkliste aus Abschnitt 6.5, Tabelle 6.1, im Rahmen dieses Beispiels zu erweitern und auf Bahnübergänge anzupassen, werden drei Quellen herangezogen: Das Projekt *Safer European Level Crossing Appraisal and Technology (SELCAT)*, das Projekt *Rail Optimisation Safety Analysis (ROSA)* und die *Eisenbahn-Bau- und Betriebsordnung (EBO)*.
Da ein Analyst meist sehr konkret für seinen betrachteten Fall (Gefährdung) denkt, ist es einfacher für ihn, zuerst konkrete Subfunktionen der Barrieren zu benennen, anstatt direkt auf abstraktere Top-Level-Funktionen oder gar Strategien zu gehen. Aus diesem Grund sind Subfunktionen für die Analyse hilfreich und sollen im Folgenden in der Checkliste ergänzt werden. Dazu werden die Funktionen aus Tabelle 6.1 weiter untergliedert. Je nach betrachtetem System und betrachteter Systemebene kann eine weitere Untergliederung der Subfunktionen hilfreich sein. Hier kann der Analyst die Checklisten seinen Bedürfnissen anpassen. Für das hier betrachtete Anwendungsbeispiel reichen zwei Ebenen, Funktionen und Subfunktionen, aus.

Projekt SELCAT

Aus dem Projekt SELCAT [LKEK+08] stammt die folgende Liste, die allgemeine (Kategorien von) Funktionen am Bahnübergang enthält.

- „Road side functions“ – Straßenseitige Funktionen[2]
  - „Road side information“ – Straßenverkehrsteilnehmer informieren (z. B. Andreaskreuz)
  - „Physical protection of road users“ – Straßenverkehrsteilnehmer physisch schützen (z. B. Schranken)
  - „Road users warning“ – Straßenverkehrsteilnehmer warnen (akustisch, visuell, physisch)
  - „Road vehicle detection“ – Straßenverkehrsteilnehmer detektieren (z. B. Videokamera, Radar)
- „Rail side function“ – Schienenseitige Funktionen
  - „Train detection“ – Züge detektieren (z. B. Achszähler)
  - „Railway side information“ – Eisenbahnpersonal informieren (z. B. Schilder)
  - „Visual train warning“ – Züge (Tf) visuell warnen (z. B. Lichtsignale)
  - „Physical train protection“ – Züge physisch sichern (z. B. automatische Zugsicherung (ATP), induktive Zugsicherung (INDUSI))
- Sonstige
  - „Information to central control room“ – Zentralen Kontrollraum informieren (z. B. Videokamera, Telefon)

Um die Checkliste zu vervollständigen, soll geprüft werden, ob alle diese Funktionen in der Checkliste enthalten sind. Wenn nicht, werden sie einer Strategie zugeordnet und ergänzt. Im Rahmen des SELCAT-Projekts wurden für diese Funktionen auch Implementierungsbeispiele gegeben [TOSW09].
Eine Zuordnung zwischen den SELCAT-Funktionen und der Checkliste aus Tabelle 6.1 ist in Tabelle 9.1 aufgeführt. Dabei sind einige der SELCAT-Funktionen Subfunktionen der Funktionen aus Tabelle 6.1. Dies wird durch die Schreibweise „Funktion: Subfunktion“ dargestellt, z. B. „informieren, warnen: Straßenverkehrsteilnehmer informieren“.

[2] Zitate aus [LKEK+08], übersetzt durch die Autorin

Projekt ROSA

Das Projekt ROSA listet in [GHGP09b] die folgenden Barrieren für Bahnübergänge:

- „Barrier: track occupancy detection on LC[3]
- Barrier: activation of train announcement on LC
- Barrier: LC Protection
- Barrier: check of LC protection
- Barrier: LC monitoring“ [GHGP09b]

Diese fünf in [GHGP09b] als funktionale Barrieren bezeichneten Punkte sind jedoch keine Barrieren. Sie stellen noch keine Umsetzung / Implementierung dar. Es sind Barrierefunktionen. Für diese als Barrieren bezeichneten Funktionen werden im Rahmen von ROSA auch ausgewählte Implementierungsbeispiele gegeben [GHGP09b].
Alle diese „Barrieren“ gehören laut [GHGP09b] zur Klasse „separation of road and track“ Diese Klasse entspricht der Strategie *2. Trennung von Energie und Ziel in Zeit und / oder Raum*.
BÜ-Sicherung (LC Protection) ist ein Sammelbegriff, unter den verschiedene Maßnahmen fallen, z. B. Andreaskreuz, Halbschranken, Lichtzeichen (Implementierungsbeispiele aus [GHGP09b]). Die BÜ-Sicherung wird in ROSA zusammengefasst als nur eine „Barriere“ betrachtet, was auch dem Sprachgebrauch der Eisenbahnen entspricht.
Bei der Auflistung der „Barrieren“ ist auffällig, dass Teile der BÜ-Sicherung, nämlich ihre Aktivierung (track occupancy detection on LC, activation of train announcement on LC) und ihre Prüfung / Überwachung (check of LC protection) als eigene „Barrieren“ hervorgehoben werden. Die Umsetzungen der Aktivierung und Überwachung der BÜ-Sicherung sind klassisch gesehen Barrieren, denn sie entsprechen der Definition einer Barriere nach Sklet [Skl06]: Sie sind physische und / oder nichtphysische Mittel, die geplant wurden, um unerwünschte Ereignisse oder Unfälle zu vermeiden, zu beherrschen oder abzumildern (siehe Abschnitt 2.3.1). Allerdings sind sie voneinander funktional abhängig: Eine Aktivierung der BÜ-Sicherung ist ohne die eigentliche BÜ-Sicherung wirkungslos und umgekehrt. Andererseits sind Aktivierung und Deaktivierung notwendig, um Barrieren, die z. B. aus betrieblichen Gründen nicht immer aktiv sein sollen, zu steuern.
Die Überwachung von Barrieren (check of LC protection) ist ein bei der Eisenbahn viel verwendetes Prinzip. Es dient der Verbesserung der Sicherheit der Barriere.
Die Gefahrraumfreimeldung (LC monitoring) ist eine „Barriere“, die in Deutschland nur bei Bahnübergängen mit Schranken verwendet wird. Der im Beispiel betrachtete BÜ besitzt Halbschranken und daher keine Gefahrraumfreimeldung. Dennoch wird diese „Barriere“ als Funktion in die Checkliste aufgenommen, um die Qualität der Checkliste zu verbessern und sie auch für die Untersuchung anderer Bahnübergangstypen nutzbar zu machen.

Tabelle 9.1: Checkliste zur Bestimmung von Barriere-Funktions-Paaren für den Bereich Eisenbahn, ergänzt um SELCAT-Funktionen und ROSA-Barrieren für Bahnübergänge

Strategie	Funktion	Barriere / Umsetzung
1. Reduzieren der Energiemenge	Fahrzeuggeschwindigkeit reduzieren	Geschwindigkeitsbeschränkung (durch Schilder oder Signale), Geschwindigkeitsüberwachung / Zugbeeinflussung
2. Trennung von Energie und Ziel in Zeit und / oder Raum	betriebliche Regeln aufstellen	betriebliche Regeln zum Abstand Halten (Zugleitbetrieb, StVO)
	betriebliche Regeln aufstellen: Reihenfolge festlegen	Vorfahrtsregeln (StVO)
	Wartepositionen festlegen	Signale und Tafeln im Bahnhof

[3]Level Crossing (Anmerkung der Autorin)

Tabelle 9.1: Checkliste zur Bestimmung von Barriere-Funktions-Paaren für den Bereich Eisenbahn, ergänzt um SELCAT-Funktionen und ROSA-Barrieren für Bahnübergänge (Fortsetzung)

Strategie	Funktion	Barriere / Umsetzung
	Arbeit so gestalten, dass das Ziel nicht so nah an die Energiequelle heran muss	Bedienung per Fernsteuerung (Rangieren)
	Wege freigeben / verwehren: Straßenverkehrsteilnehmer warnen, BÜ-Sicherung, Prüfung der BÜ-Sicherung	visuell: Lichtzeichen für den Straßenverkehr am BÜ, Schranken, Halbschranken; akustisch: Glocke am BÜ, Horn / Pfeife des Zuges
	Wege freigeben / verwehren: Züge (Tf) visuell warnen	(Licht-)Signalanlagen (Hauptsignale, Überwachungssignale
	Wege freigeben / verwehren: Züge physisch sichern / BÜ-Sicherung, Prüfung der BÜ-Sicherung	Zugbeeinflussung (ATP, INDUSI), Prüfung durch Stellwerk, Prüfung durch Personal
	betreten von Gleisanlagen verbieten	Verkehrsregeln (StVO)
	bewegliche Objekte detektieren: Straßenverkehrsteilnehmer detektieren / Gefahrraumfreimeldung, BÜ beobachten/überwachen	Videokameras, Radar
	bewegliche Objekte detektieren: Züge detektieren / Aktivierung der Ankündigung des Zuges am BÜ, Gleisbelegt-Erkennung am BÜ	Achszähler, Gleisstromkreise
	energiegeladene Gegenstände außer Reichweite von Personen halten	hohe Elektrifizierung / Oberleitungen
	Ausweichmöglichkeiten / Fluchtmöglichkeiten bieten	Halbschranken
	Verkehrswege trennen	zweites Gleis
	BÜ entfernen	Umbau
	Neubau von BÜ verhindern	Bauvorschriften, Baupläne
3. Isolierung durch Einfügen materieller Barrieren	Umgebung gestalten	Topographie des Geländes, stabile Hülle (Steifigkeit des Wagenkastens), unterirdische Verkabelung, Gehäuse von Bahnanlagen
	Gefahrenbereich absperren, Straßenverkehrsteilnehmer physisch schützen, BÜ-Sicherung, Prüfung der BÜ-Sicherung	Absperrungen, Schranken, Tore, Rampen
4. Verändern von Oberflächen, an denen man sich verletzen kann	abrunden von Ecken und Kanten	abgerundete Sitzkanten, Griffe
	weichmachen von Kontaktflächen	schaumstoffummantelte Stangen, gepolsterte Sitze, Gummikanten an Türen

Tabelle 9.1: Checkliste zur Bestimmung von Barriere-Funktions-Paaren für den Bereich Eisenbahn, ergänzt um SELCAT-Funktionen und ROSA-Barrieren für Bahnübergänge (Fortsetzung)

Strategie	Funktion	Barriere / Umsetzung
5. Stärken des Ziels, um der Energie standzuhalten	Schutzkleidung tragen	Handschuhe
6. Schulung von Menschen zum Verhindern, dass Energie freigesetzt wird	informieren, warnen: Straßenverkehrsteilnehmer informieren	visuell: Andreaskreuz, Baken; physisch: Rüttelstreifen auf der Straße
	informieren, warnen: Eisenbahnpersonal informieren	Schilder: Signaltafeln
	informieren, warnen: zentralen Kontrollraum informieren	Videokameras, Telefon
	unterrichten, Regeln aufschreiben und zugänglich machen, spezielle Prozeduren / Notfallmaßnahmen schulen	spezielle Prozeduren (z. B. Fahrdienstvorschrift, Straßenverkehrsordnung)
	Verhalten üben	Sicherheitstraining (Ausbildung der Tf, Fahrschule)

Aus diesen Beispielen (SELCAT und ROSA) ist ersichtlich, dass in vielen Projekten immer wieder die gleiche Arbeit geleistet wird, meist mit leicht unterschiedlichem Fokus und das Ergebnis mit leicht unterschiedlicher Formulierung. Es ist wünschenswert, diese Arbeiten zu vereinheitlichen und dann in einer Form zu veröffentlichen, die eine weitere Nutzung unterstützt. Eine gut geeignete Form der Veröffentlichung für eine solche Arbeit wäre eine internationale Norm, z. B. nach dem Vorbild der E DIN EN 15380-4 [DIN09], da Normen im Ingenieurbereich einen hohen Stellenwert und einen großen Verbreitungsgrad haben. Projektberichte wie die von SELCAT oder ROSA hingegen sind trotz zahlreicher Veröffentlichungen in Zeitschriften und auf Konferenzen weniger bekannt.

Eisenbahn-Bau- und Betriebsordnung

In der Eisenbahn-Bau- und Betriebsordnung (EBO) [Bun12] ist vorgeschrieben, wie Bahnübergänge gesichert werden müssen, in Abhängigkeit von verschiedenen Parametern wie z. B. der Verkehrsstärke. Die EBO nennt dabei technische Mittel, die verwendet werden müssen, oder Menschen als Ausführende von Maßnahmen. Dies sind Barrieren (Implementierung der Barrieremechanismen).
Tabelle 9.2 enthält die Barrieren am Bahnübergang aus der EBO zusammen mit dem Paragraphen, in dem sie genannt werden. Die Barrieren wurden um Funktionen und Subfunktionen ergänzt und den Strategien zugeordnet.
Anmerkung: In einigen Fällen erlaubt die EBO nur den Einsatz bestimmter Kombinationen von Barrieren.
Neben der EBO enthält auch die Verordnung über den Bau und Betrieb der Straßenbahnen (BOStrab) Vorschriften zur Sicherung von Bahnübergängen. Diese Vorschriften unterscheiden sich von denen der EBO. Der in diesem Beispiel betrachtete Bahnübergang mit Überwachungssignal kommt in dieser Form nur bei Vollbahnen, nicht aber bei Straßenbahnen vor. Daher soll die BOStrab an dieser Stelle nicht für die Vorbereitung der Checklisten genutzt werden. Es ist nicht zu erwarten, dass sich dadurch die Vollständigkeit der Analyse erhöhen würde.

Tabelle 9.2: Strategien, Funktionen und Barrieren der EBO für die Sicherheit an Bahnübergängen

Strategie	Funktion	Subfunktion	Barriere / Umsetzung	EBO-§
1. Reduzieren der Energiemenge	Fahrzeuggeschwindigkeit reduzieren	Geschwindigkeit beschränken	max. 160 km/h an BÜ	§ 11 (2)
			Geschwindigkeitsbeschränkung (Vorschrift oder Schild)	§ 11 (7)
2. Trennung von Energie und Ziel in Zeit und / oder Raum	Verkehrswege räumlich trennen	Verkehrswege von Straßenverkehr und Schienenverkehr trennen	Bauvorschrift: Verbot von BÜ auf Strecken mit einer zugelassenen Geschwindigkeit von mehr als 160 km/h	§ 11 (2)
	Wege freigeben / verwehren		Lz	§ 11 (6)
			Blinklichter	§ 11 (6)
			Halbschranken	§ 11 (6)
			Schranken	§ 11 (6)
			Posten	§ 11 (3), § 11 (11)
			hörbare Zeichen	§ 11 (15)
			Abschlüsse	§ 11 (10) a)
			Abschlüsse mit Sprechanlage	§ 11 (10) b)
		Straßenverkehrsteilnehmer warnen	hörbare Signale der Eisenbahnfahrzeuge	§ 11 (7)
	bewegliche Objekte detektieren	Züge detektieren: Straßenverkehrsteilnehmern die Möglichkeit geben, Züge zu sehen	Übersicht	§ 11 (7), § 11 (9), § 11 (10)
		Straßenverkehrsteilnehmer detektieren	technische Einrichtung, die das Freisein des Bahnübergangs feststellt	§ 11 (16)
			Sicht des Schrankenwärters	§ 11 (15)
	Ablauf verlangsamen, um den Menschen Zeit zu geben, die Situation richtig einzuschätzen	Radfahrer zum Absteigen und Durchschieben zwingen [FMS05]	Umlaufsperren	§ 11 (9)
		Geschwindigkeit beschränken	Geschwindigkeitsbeschränkung (Vorschrift oder Schild)	§ 11 (7)

Tabelle 9.2: Strategien, Funktionen und Barrieren der EBO für die Sicherheit an Bahnübergängen (Fortsetzung)

Strategie	Funktion	Subfunktion	Barriere / Umsetzung	EBO-§
	Aufmerksamkeit lenken	Blickrichtung der Straßenverkehrsteilnehmer in jede Richtung der Strecke lenken [FMS05]	Umlaufsperren	§ 11 (9)
	Gefahrenbereich verkleinern		nur ein Gleis	§ 11 (7)
3. Isolierung durch Einfügen materieller Barrieren	Gefahrenbereich absperren		Halbschranken	§ 11 (6)
			Schranken	§ 11 (6)
			Abschlüsse	§ 11 (10)
			Abschlüsse mit Sprechanlage	§ 11 (10)
6. Schulung von Menschen zum Verhindern, dass Energie freigesetzt wird	Straßenverkehrsteilnehmer informieren / warnen		Andreaskreuz	§ 11 (3)
			Kennzeichnung von Privatwegen ohne öffentlichen Verkehr	§ 11 (3)
			Schild „Hafengebiet, Schienenfahrzeuge haben Vorrang“ an den Einfahrten zum Gebiet	§ 11 (5)
			Schild „Industriegebiet, Schienenfahrzeuge haben Vorrang“ an den Einfahrten zum Gebiet	§ 11 (5)

Bahnübergang gesamt

Um eine geeignete Checkliste für die Analyse zu erhalten, müssen die Checklisten aus den verschiedenen Quellen

- Abschnitt 6.5 (Tabelle 6.1)
- SELCAT (Tabelle 9.1)
- ROSA (Tabelle 9.1)
- EBO (Tabelle 9.2)

zu einer Checkliste zusammengefügt werden. Dabei sollte vermieden werden, Funktionen, Subfunktionen oder Barrieren doppelt aufzuführen – auch nicht unter ähnlichen Bezeichnungen. Dies würde die Arbeit mit der Checkliste erschweren. Tabelle 9.3 enthält die zusammengefügte Checkliste. In der Tabelle sind die Quellen der Barrieren und Funktionen durch Farben markiert: lila = SELCAT, magenta = ROSA, orange = EBO. Werden Barrieren oder Funktionen in mehreren Quellen genannt, werden sie nur entsprechend einer Quelle farbig markiert.
Anhand der Färbungen ist zu sehen, dass die Projekte SELCAT und ROSA Funktionen beschreiben, während die EBO die konkrete Umsetzung, d. h. die Barrieren behandelt.

Tabelle 9.3: Checkliste zur Bestimmung von Barriere-Funktions-Paaren für den Bereich Eisenbahn, ergänzt um Funktionen und Barrieren aus SELCAT, ROSA und der EBO für Bahnübergänge

Strategie	Funktion	Subfunktion	Barriere / Umsetzung
1. Reduzieren der Energiemenge	Fahrzeuggeschwindigkeit reduzieren	Geschwindigkeit für Züge beschränken	Geschwindigkeitsbeschränkung für Züge (durch Vorschrift, Schild oder Signal)
			max. 160 km/h an BÜ
		Geschwindigkeit der Züge überwachen und bei Bedarf reduzieren	Zugbeeinflussung (ATP, z. B. PZB, INDUSI, LZB)
2. Trennung von Energie und Ziel in Zeit und / oder Raum	betriebliche Regeln aufstellen	betriebliche Regeln zum Abstand Halten aufstellen	Zugleitbetrieb, StVO
		Reihenfolge festlegen	Verkehrsregel bzgl. Vorrang des Eisenbahnverkehrs, Vorfahrtsregeln (StVO)
		Betreten von Gleisanlagen verbieten	Verkehrsregeln (StVO)
	Wartepositionen festlegen		Signale und Tafeln im Bahnhof
	Arbeit so gestalten, dass das Ziel nicht so nah an die Energiequelle heran muss		Bedienung per Fernsteuerung (Rangieren)
	Verkehrswege räumlich trennen	Verkehrswege von Straßenverkehr und Schienenverkehr trennen	Bauvorschrift: Verbot von BÜ auf Strecken mit einer zugelassenen Geschwindigkeit von mehr als 160 km/h
		BÜ entfernen	Umbau
		Neubau von BÜ verhindern	Bauvorschriften, Baupläne
		Verkehrswege des Schienenverkehrs trennen	zweites Gleis

Tabelle 9.3: Checkliste zur Bestimmung von Barriere-Funktions-Paaren für den Bereich Eisenbahn, ergänzt um Funktionen und Barrieren aus SELCAT, ROSA und der EBO für Bahnübergänge (Fortsetzung)

Strategie	Funktion	Subfunktion	Barriere / Umsetzung
	Wege freigeben / verwehren	Straßenverkehrsteilnehmer warnen / BÜ-Sicherung, Prüfung der BÜ-Sicherung	Lz, Blinklichter, Schranken, Halbschranken, Abschlüsse, Abschlüsse mit Sprechanlage, Posten, hörbare Zeichen, z. B. Glocke am BÜ, hörbare Signale der Eisenbahnfahrzeuge, z. B. Horn oder Pfeife des Zuges
		Züge (Tf) visuell warnen	(Licht-)Signalanlagen (Hauptsignale, Überwachungssignale)
		Züge physisch sichern / BÜ-Sicherung, Prüfung der BÜ-Sicherung	Zugbeeinflussung (ATP, z. B. PZB, INDUSI, LZB), Prüfung durch Stellwerk, Prüfung durch Personal
	bewegliche Objekte detektieren	Straßenverkehrsteilnehmer detektieren / Gefahrraumfreimeldung, BÜ beobachten / überwachen	Videokameras, Radar, technische Einrichtungen, die das Freisein des BÜ feststellen, Sicht des Schrankenwärters
		Züge detektieren / Aktivierung der Ankündigung des Zuges am BÜ, Gleisbelegt-Erkennung am BÜ	Achszähler, Gleisstromkreise
		Straßenverkehrsteilnehmern die Möglichkeit geben, Züge zu sehen	Übersicht
	Energiequelle außer Reichweite von Personen halten		hohe Elektrifizierung / Oberleitungen
	Ausweich- / Fluchtmöglichkeiten bieten		Halbschranken

Tabelle 9.3: Checkliste zur Bestimmung von Barriere-Funktions-Paaren für den Bereich Eisenbahn, ergänzt um Funktionen und Barrieren aus SELCAT, ROSA und der EBO für Bahnübergänge (Fortsetzung)

Strategie	Funktion	Subfunktion	Barriere / Umsetzung
	Aufmerksamkeit lenken	Blickrichtung der Straßenverkehrsteilnehmer in jede Richtung der Strecke lenken [FMS05]	Umlaufsperren
	Ablauf verlangsamen, um den Menschen Zeit zu geben, die Situation richtig einzuschätzen	Radfahrer zum Absteigen und Durchschieben zwingen [FMS05]	Umlaufsperren
		Geschwindigkeit für Züge beschränken	max. 160 km/h an BÜ, Geschwindigkeitsbeschränkung für Züge (durch Vorschrift, Schild oder Signal (inkl. Geschwindigkeitsüberwachung))
		Geschwindigkeit für Straßenverkehrsteilnehmer beschränken	Verkehrsschild
	Gefahrenbereich verkleinern		nur ein Gleis am BÜ
3. Isolierung durch Einfügen materieller Barrieren	Umgebung gestalten	Topographie des Geländes gestalten	Bahndamm, Zäune, Brücken, Tunnel
		Gefahrenbereich absperren, Straßenverkehrsteilnehmer physisch schützen, BÜ-Sicherung, Prüfung der BÜ-Sicherung	Halbschranken, Schranken, Abschlüsse, Abschlüsse mit Sprechanlage, Absperrungen, Tore, Rampen
		gefährliche Gegenstände vergraben / einschließen	unterirdische Verkabelung, Gehäuse von Bahnanlagen
	Fahrzeuge gestalten		stabile Hülle (Steifigkeit des Wagenkastens)

Tabelle 9.3: Checkliste zur Bestimmung von Barriere-Funktions-Paaren für den Bereich Eisenbahn, ergänzt um Funktionen und Barrieren aus SELCAT, ROSA und der EBO für Bahnübergänge (Fortsetzung)

Strategie	Funktion	Subfunktion	Barriere / Umsetzung
4. Verändern von Oberflächen, an denen man sich verletzen kann	abrunden von Ecken und Kanten		abgerundete Sitzkanten, Griffe
	weichmachen von Kontaktflächen		schaumstoffummantelte Stangen, gepolsterte Sitze, Gummikanten an Türen
5. Stärken des Ziels, um der Energie standzuhalten	Schutzkleidung tragen		Handschuhe
6. Schulung von Menschen zum Verhindern, dass Energie freigesetzt wird	informieren, warnen	Straßenverkehrsteilnehmer informieren	Andreaskreuz, Baken, Kennzeichnung von Privatwegen ohne öffentlichen Verkehr, Schild „Hafengebiet, Schienenfahrzeuge haben Vorrang“, Schild „Industriegebiet, Schienenfahrzeuge haben Vorrang“ an den Einfahrten zum Gebiet, Rüttelstreifen auf der Straße
		Eisenbahnpersonal informieren	Signaltafeln, Bahnübergangstafel (Zs 9), Rautentafeln (Bü 2), Warntafel (So 15), BÜ-Ankündetafeln, BÜ-Kennzeichentafeln
		zentralen Kontrollraum informieren	Videokameras, Telefon
	unterrichten, spezielle Prozeduren / Notfallmaßnahmen schulen	Straßenverkehrsteilnehmer unterrichten	Fahrschule
		Eisenbahnpersonal unterrichten	Ausbildungsbetrieb, Berufsschule
	Regeln aufschreiben und zugänglich machen	Regeln / Prozeduren für Straßenverkehr	StVO
		Regeln / Prozeduren für Eisenbahnverkehr	Fahrdienstvorschrift
	Verhalten üben		Sicherheitstraining (Ausbildung der Tf, Vorschriften über abzuleistende Mindeststunden (Fahrpraxis)), Fahrschule, Fahrsicherheitstraining

C2: Nutzung der Checklisten

Bestimmung der Funktionen für die Barrieren aus Schritt B

Für das Beispiel des betrachteten Bahnübergangs werden für die Barrieren aus der FTA (siehe Abschnitt 9.2) die zugehörigen Funktionen bestimmt. Dazu wird die für Bahnübergänge angepasste Checkliste aus Tabelle 9.3 verwendet. Jede identifizierte Barriere wird in der Tabelle gesucht und dann werden die Funktionen und Strategien links daneben abgelesen. Doch die Funktionen dürfen nicht unreflektiert übernommen werden. Es muss geprüft werden, ob die Barriere im betrachteten Fall diese Funktion wirklich hat.
Im Fehlerbaum (Abbildung 9.1) wurden in Schritt B fünf Barrieren identifiziert: gelbe Lichtzeichen (Lz), rote Lz, Halbschranken, Überwachungssignal und PZB-Magnet.
Die **gelben und roten Lz** sind in Tabelle 9.3 der Funktion *Wege freigeben / verwehren* der Strategie *2. Trennung von Energie in Zeit und / oder Raum* zugeordnet. Die zugehörige Subfunktion ist *Straßenverkehrsteilnehmer warnen* (SELCAT) im Rahmen der *BÜ-Sicherung* (ROSA).
Im Projekt SELCAT wurden zugunsten einer internationalen Vergleichbarkeit, die im Hauptfokus des Projekts stand, generische Formulierungen und somit breite Definitionen für Funktionen verwendet. Dadurch lassen sich die Konzepte aller untersuchten Länder diesen Funktionen zuordnen. Dies gilt auch für die Funktion *Straßenverkehrsteilnehmer warnen* (siehe S. 106).
Die Lichtzeichen am Bahnübergang (BÜ) sind allerdings nicht nur eine Warnung wie „Sei vorsichtig!“. Zumindest in Deutschland haben sie den Charakter einer Aufforderung, etwas Bestimmtes zu tun: § 19 (2) Straßenverkehrs-Ordnung (StVO): „Fahrzeuge haben vor dem Andreaskreuz, Fußgänger in sicherer Entfernung vor dem Bahnübergang zu warten, wenn [...] gelbe oder rote Lichtzeichen gegeben werden“ [Bun10]. Im Projekt ROSA wird das ähnlich gesehen: Dort sind die Lichtzeichen als „stop light“ bezeichnet, und sie dienen zur „optical indication of prohibited access onto LC (due to approaching train)“ [GHGP09b]. Daher wird die Formulierung von SELCAT für die Subfunktion der Barrieren gelbe und rote Lz ersetzt durch: *Straßenverkehrsteilnehmer zum Warten vor dem BÜ auffordern*. Diese Subfunktion ist in der Checkliste so noch nicht enthalten und wird zur Ergänzung der Checkliste vorgemerkt.
Die Barriere **Halbschranken** dient dazu, den Straßenverkehrsteilnehmern den Durchgang zum BÜ zu versperren. In Tabelle 9.3 treten die Halbschranken mehrfach auf: Zwei Mal im Rahmen der Strategie 2 und ein Mal im Rahmen der Strategie 3. Wie auch die Lichtzeichen haben die Halbschranken die Subfunktion *Straßenverkehrsteilnehmer warnen / BÜ-Sicherung*. Wie dort soll auch bei den Halbschranken der Formulierung *Straßenverkehrsteilnehmer zum Warten vor dem BÜ auffordern* der Vorrang gegeben werden. Weiterhin dienen die Halbschranken auch der Funktion *Ausweich-/ Fluchtmöglichkeit bieten* der Strategie 2. Diese Funktion wirkt jedoch nicht gegen die betrachtete Gefährdung „Zug befährt ungesicherten BÜ“. Daher wird diese Funktion nicht mit in die Liste der B-F-Paare aufgenommen. Als dritte Funktion setzen die Halbschranken auch die Subfunktion *Gefahrenbereich absperren, Straßenverkehrsteilnehmer physisch schützen, BÜ-Sicherung* der Funktion *Umgebung gestalten*, Strategie 3, um. Diese Funktion wirkt, wie die erste, gegen die betrachtete Gefährdung und ist daher im Rahmen der Analyse relevant.
Das **Überwachungssignal** hat ebenfalls die Funktion *Wege freigeben / verwehren* (Strategie 2), allerdings hier mit der Subfunktion *Züge (Tf) visuell warnen*.
Die Barriere **PZB-Magnet** ist in Tabelle 9.3 nicht direkt enthalten. Stattdessen ist die gesamte PZB (d. h. streckenseitiger und fahrzeugseitiger Anteil) unter dem Punkt Zugbeeinflussung aufgeführt. Zu dieser Barriere gehören die Subfunktion *Züge physisch sichern / BÜ-Sicherung* und die Funktion *Wege freigeben / verwehren* der Strategie 2. Die PZB setzt außerdem die Funktion *Fahrzeuggeschwindigkeit reduzieren* der Strategie *1. Reduzieren der Energiemenge* um. Für die betrachtete Gefährdung ist diese Funktion jedoch nur hilfreich, wenn die Geschwindigkeit so weit reduziert wird, dass das Fahrzeug vor dem BÜ zum Stehen kommt. Dieser Fall ist über die Strategie 2 abgedeckt, daher wird die Funktion *Fahrzeuggeschwindigkeit reduzieren* nicht in die Liste der B-F-Paare aufge-

nommen.
Alle mit Hilfe der FTA identifizierten B-F-Paare sind in Tabelle 9.4 zusammen mit den zugehörigen Subfunktionen und Strategien aufgeführt.

Tabelle 9.4: B-F-Paare aus dem Fehlerbaum, ergänzt um Strategien und Subfunktionen; **fett gedruckt**: neue Punkte zur Ergänzung der Checkliste

Strategie	Funktion	Subfunktion	Barriere
2. Trennung von Energie und Ziel in Zeit und / oder Raum	Wege freigeben / verwehren	Züge physisch sichern / BÜ-Sicherung	PZB(-Magnet)
		Straßenverkehrsteilnehmer zum Warten vor dem BÜ auffordern	**gelbe Lz**
			rote Lz
			Halbschranken
		Züge (Tf) visuell warnen	Überwachungssignal
3. Isolierung durch Einfügen materieller Barrieren	Umgebung gestalten	Gefahrenbereich absperren, Straßenverkehrsteilnehmer physisch schützen, BÜ-Sicherung	Halbschranken

Identifikation weiterer Barriere-Funktions-Paare

Gemäß der Beschreibung von Schritt C (Abschnitt 6.5) wird nun geprüft, ob es im System noch weitere B-F-Paare gibt, die bei der durchgeführten FTA nicht identifiziert wurden. Dazu wird die Checkliste aus Tabelle 9.3 verwendet. Hierbei ist zu beachten, dass der Fehlerbaum aus Abbildung 9.1 aufgrund der gewählten Sichtweise eines Herstellers nur einen Teil des Systems umfasst. Daher sollten bei der Suche nach weiteren B-F-Paaren insbesondere die Systemelemente berücksichtigt werden, die im FT nicht enthalten sind.
Zunächst wird für alle in der Checkliste vorhandenen Strategien gefragt: Wird diese Strategie im betrachteten System verwendet? Um die Prüfung zu vereinfachen und zu beschleunigen, wird zunächst gefragt, ob die Strategie gegen die zu untersuchende Gefährdung überhaupt wirksam sein kann. Dies ist ein Vorgriff auf die Wirksamkeits-Prüfung aus Schritt D.
Die **Strategien 2 und 3** aus Tabelle 9.3 werden am betrachteten BÜ verwendet. Dies hat Schritt B ergeben – entsprechende B-F-Paare sind in Tabelle 9.4 vorhanden. Die Strategien 2 und 3 sind also gegen die zu untersuchende Gefährdung wirksam. Trotz der bereits identifizierten B-F-Paare sollte an dieser Stelle geprüft werden, ob zu jeder dieser Strategien alle relevanten implementierten Funktionen und Barrieren bzgl. der Gefährdung „Zug befährt ungesicherten BÜ“ identifiziert wurden. Werden am betrachteten BÜ noch weitere Funktionen / Barrieren der Strategie *2. Trennung von Energie und Ziel in Zeit und / oder Raum* verwendet? Ja, die Funktion *bewegliche Objekte detektieren*, Subfunktion *Aktivierung der Ankündigung des Zuges am BÜ*. Als mögliche Barrieren sind in Tabelle 9.3 Achszähler und Gleisstromkreise angegeben. Keine dieser Barrieren bzw. ihre Umsetzung ist in der Systembeschreibung des Beispiel-BÜ aus Abschnitt 8.2 enthalten. Im Beispiel-BÜ wird diese Barriere als *Einschaltkontakt* bezeichnet. Der Einschaltkontakt ist im Fehlerbaum aus Abbildung 9.1 enthalten, wurde in Schritt B aber nicht als Barriere identifiziert. Warum das so ist, wird in Schritt D erläutert. Da der Begriff Einschaltkontakt in Tabelle 9.3 nicht enthalten ist, wird er zur Ergänzung vorgemerkt. Die Funktion *bewegliche Objekte detektieren* aus Tabelle 9.3 hat noch eine weitere Subfunktion, die am BÜ zum Einsatz kommt: *Straßenverkehrsteilnehmer detektieren / Gefahrraumfreimeldung, BÜ beobachten / überwachen*. Allerdings ist keine der in Tabelle 9.3 aufge-

führten Barrieren / Umsetzungen am betrachteten BÜ vorhanden. Dennoch wird der BÜ beobachtet, und zwar vom Triebfahrzeugführer (Tf).
Der Tf kommt in Tabelle 9.3 in der Spalte Barriere / Umsetzung nicht direkt vor. Dennoch ist er Teil vieler Barrieren, wie z. B. der Barriere Überwachungssignal, denn er setzt diese visuellen Informationen in die Tat um (siehe auch Abschnitt 3.2.7). Die Rolle des Tf im Eisenbahnsystem ist komplex und Gegenstand zahlreicher Forschungen zum Thema Human Factors, siehe z. B. [Ham11]. Die Rolle des Tf als Umsetzer der Informationen soll an dieser Stelle nicht betrachtet werden, Betrachtet wird hier nicht, ob der Tf das Halt zeigende Überwachungssignal übersieht. Die Barriere / Funktion, die an dieser Stelle angesprochen wird, ist die Möglichkeit der Gefahrenabwehr durch den Tf. Er könnte einen ungesicherten Bahnübergang erkennen und seinen Zug rechtzeitig zum Stehen bringen. Der Tf erfüllt in diesem Fall die Funktion, die Strecke vor ihm zu beobachten. Er kann dabei z. B. Straßenverkehrsteilnehmer auf dem BÜ entdecken – und möglicherweise den Zug noch rechtzeitig zum Stehen bringen. Über die Stärke dieser Barriere, die Wahrscheinlichkeit, mit der dem Tf diese Gefahrenabwehr gelingt, soll an dieser Stelle nicht eingegangen werden. Es genügt, dass die prinzipielle Möglichkeit besteht. Man könnte an dieser Stelle noch die Frage stellen, ob diese Barriere Tf mit berücksichtigt werden darf, da eine Barriere nach Sklet [Skl06] ein Mittel ist, das *geplant* wurde, um Unfälle zu vermeiden. Zweifellos wurde der Tf als Teil des Systems Eisenbahn geplant. Es gehört zu seinen Aufgaben, die Strecke vor ihm zu beobachten und auf gefährliche Situationen zu reagieren. Dazu steht ihm die Möglichkeit einer Schnellbremsung zur Verfügung. Es kann also davon ausgegangen werden, dass diese Möglichkeit der Gefahrenabwehr geplant wurde und daher darf sie als Barriere betrachtet werden. Da der Tf in Tabelle 9.3 bei der Subfunktion *Straßenverkehrsteilnehmer detektieren / Gefahrraumfreimeldung, BÜ beobachten / überwachen* noch nicht aufgeführt ist, wird dieser Punkt zur Ergänzung vorgemerkt.
Auch auf Seite der Straßenverkehrsteilnehmer wird die Strategie 2 verwendet, z. B. die Funktion *Ausweich- Fluchtmöglichkeiten bieten*. Diese Funktionen sind jedoch nicht relevant für die Gefährdung „Zug befährt ungesicherten BÜ“. Ebenso verhält es sich mit der Funktion *Gefahrenbereich verkleinern*. Sie ist am betrachteten BÜ zwar implementiert, da er nur ein Gleis hat, aber auch sie wirkt der betrachteten Gefährdung nicht entgegen.
Werden am BÜ außer den bereits identifizierten B-F-Paaren noch weitere Funktionen / Barrieren der Strategie *3. Isolierung durch Einfügen materieller Barrieren* verwendet? Die Antwort ist Nein.
Für die **Strategien 1, 4, 5 und 6** aus Tabelle 9.3 wurden mit Hilfe der FTA keine Barrieren identifiziert. Auch für diese Strategien wird geprüft, ob ihre Funktionen am Beispiel-BÜ verwendet werden.
Die Strategie *1. Reduzieren der Energiemenge* mit ihrer Funktion *Fahrzeuggeschwindigkeit reduzieren* kann gegen die Gefährdung „Zug befährt ungesicherten BÜ“ nur dann wirksam sein, wenn die Geschwindigkeit des Zuges bis zum Stillstand reduziert wird. Da dieser Sonderfall unter der Strategie 2 behandelt wird (siehe oben), ermöglicht es die Strategie 1 nicht, die Gefährdung „Zug befährt ungesicherten BÜ“ zu verhindern.
Die Strategie *4. Verändern von Oberflächen, an denen man sich verletzen kann*, kann die Gefährdung „Zug befährt ungesicherten BÜ“ ebenfalls nicht verhindern.
Auch die Strategie *5. Stärken des Ziels, um der Energie standzuhalten*, wirkt nicht gegen die betrachtete Gefährdung, sondern erst gegen ihre möglichen Folgen.
Die Strategie *6. Schulung von Personal zum Verhindern, dass Energie freigesetzt wird*, kann prinzipiell gegen die betrachtete Gefährdung wirksam sein. Hier ist eine detailliertere Prüfung notwendig. Die Funktion *informieren, warnen* mit der Subfunktion *Eisenbahnpersonal informieren* wird am betrachteten BÜ verwendet, in Form der *Rautentafel* (Signal Bü 2: Ein Überwachungssignal ist zu erwarten.). Die Rautentafel kennzeichnet zudem den Anfang der Einschaltstrecke des BÜ. Auch der Straßenverkehr wird durch Schilder wie Andreaskreuze und Baken informiert und gewarnt. Jedoch sind diese Straßenverkehrszeichen nicht relevant für die Gefährdung „Zug befährt ungesicherten BÜ“. Entsprechendes gilt für das Unterrichten der Straßenverkehrsteilnehmer in der Fahrschule.

Am BÜ kommt außerdem die Barriere *Ausbildungsbetrieb, Berufsschule* der Funktion *unterrichten, spezielle Prozeduren schulen* zum Einsatz. Züge werden nur von ausgebildetem Personal gefahren. Der Tf lernt im Rahmen seiner Ausbildung, die Strecke zu beobachten und im Notfall eine Bremsung auszulösen. Nach der ersten Ausbildung zum Tf folgt dann die *Fahrpraxis*. Hier wird das korrekte *Verhalten geübt*. Die geschulten *Regeln werden aufgeschrieben und (für den Tf) zugänglich gemacht*, in Form der *Fahrdienstvorschrift* (im Bereich der Deutschen Bahn die Richtlinie 408 [Deu06]). Gemäß der Richtlinie 408 [Deu06] muss ein ÜS-Bahnübergang z. B. durch Zugpersonal gesichert werden, wenn ein Zug auf der Einschaltstrecke gehalten hat oder langsamer als 20 km/h gefahren ist. Einige ÜS-BÜ-Sicherungsanlagen gehen nach Ablauf einer bestimmten Zeit (sog. Grundstellerzeit) zurück in ihre Grundstellung, d. h. die Schranken werden geöffnet und die Lichtzeichen werden ausgeschaltet.). Alle diese aufgeführten Barrieren und Funktionen sind relevant für die Gefährdung „Zug befährt ungesicherten BÜ“ und werden daher zur Liste der B-F-Paare hinzugefügt.

Die identifizierten, im System BÜ mit ÜS für die Gefährdung „Zug befährt ungesicherten BÜ“ vorhandenen Barriere-Funktionen-Paare, sind somit die 12 in Tabelle 9.5 aufgeführten.

Kleines Fazit: Bei der Identifikation von Barrieren und Funktionen mit Hilfe der Checklisten kommt es darauf an, sie zielgerichtet für die jeweilige Gefährdung zu suchen. Sonst kann es leicht zu Abschweifungen kommen.

Bei der Nutzung der Checkliste fällt auf, dass es vor allem die Barrieren und Funktionen der Strategie *6. Schulung von Personal* sind, die nicht mit Hilfe des Fehlerbaums identifiziert wurden. Das ist nicht verwunderlich, denn eine FTA ist in der Regel stark technisch orientiert. Selbst wenn menschliche Fehler mit betrachtet werden, so sind die vorbereitenden Maßnahmen wie Schulung meist nicht enthalten.

C3: Ergänzung der Checklisten

Die als Basis verwendete Checkliste (Tabelle 9.3) wird um die gefundenen Barriere-Funktions-Paare, zusammen mit Strategien und Subfunktionen aus Tabelle 9.5 ergänzt. Aus Platzgründen wird diese große Tabelle nicht an dieser Stelle, sondern im Anhang B, Tabelle B.1 aufgeführt. Diese Tabelle aus Anhang B kann als Basis für Untersuchungen anderer BÜ oder auch für die Untersuchung anderer Gefährdungen am Beispiel-Bahnübergang dienen.

9.3.2 Ergebnis

Die Ergebnisse des Schritts C sind die Liste mit Barriere-Funktions-Paaren aus Tabelle 9.5 und die ergänzte Checkliste zur weiteren Nutzung in nachfolgenden Analysen: Tabelle B.1 in Anhang B.

Im Vergleich zu Schritt B sind zu den zunächst 5 identifizierten Barrieren, die in Tabelle 9.4 zu 6 B-F-Paaren ergänzt wurden, weitere 6 hinzugekommen, die in Tabelle 9.5 blau gedruckt sind. Sie betreffen zum einen Barrieren, bei denen der Mensch mitwirkt, zum anderen den Einschaltkontakt, der im Fehlerbaum enthalten ist, aber in Schritt B nicht als Barriere identifiziert wurde (zur Erläuterung siehe auch Schritt D).

Tabelle 9.5: Barriere-Funktions-Paare für den betrachteten BÜ, ergänzt um Strategien; **fett gedruckt**: neue Punkte zur Ergänzung der Checkliste; blau: Punkte, die nicht in Schritt B identifiziert wurden

Strategie	Funktion	Subfunktion	Barriere	Nr.
2. Trennung von Energie und Ziel in Zeit und / oder Raum	Wege freigeben / verwehren	Züge physisch sichern / BÜ-Sicherung	PZB	1
		Straßenverkehrsteilnehmer zum Warten vor dem BÜ auffordern	**gelbe Lz**	2
			rote Lz	3
			Halbschranken	4
		Züge (Tf) visuell warnen	Überwachungssignal	5
	Bewegliche Objekte detektieren	Straßenverkehrsteilnehmer detektieren / Gefahrraumfreimeldung, BÜ beobachten / überwachen	**Tf**	6
		Züge detektieren / Aktivierung der Ankündigung des Zuges am BÜ	**Einschaltkontakt**	7
3. Isolierung durch Einfügen materieller Barrieren	Umgebung gestalten	Gefahrenbereich absperren, Straßenverkehrsteilnehmer physisch schützen, BÜ-Sicherung	Halbschranken	8
6. Schulung von Personal zum Verhindern, dass Energie frei gesetzt wird	Informieren, warnen	Eisenbahnpersonal informieren: Überwachungssignal ankündigen	Rautentafel (Bü 2)	9
	Unterrichten, spezielle Prozeduren / Notfallmaßnahmen schulen	Eisenbahnpersonal unterrichten	Ausbildungsbetrieb, Berufsschule	10
	Regeln aufschreiben und zugänglich machen	Regeln / Prozeduren für den Eisenbahnverkehr aufschreiben und zugänglich machen	Fahrdienstvorschrift	11
	Verhalten üben	Erlerntes auffrischen	Sicherheitstraining	12

9.4 Schritt D: Prüfen auf Wirksamkeit und Unabhängigkeit

9.4.1 Voraussetzungen

Schritt C wurde abgeschlossen. Für die betrachtete Gefährdung „Zug befährt ungesicherten Bahnübergang“ liegt eine Liste mit 12 identifizierten Barriere-Funktions-Paaren vor (Tabelle 9.5). Die in Schritt C verwendeten Checklisten wurden mit Hilfe von gesetzlichen Vorgaben und den Erkenntnissen aus mehreren Projekten vorbereitet. Daher kann davon ausgegangen werden, dass die Liste der Barriere-Funktions-Paare ein hohes Maß an Vollständigkeit hat.

9.4.2 Durchführung

In Schritt D werden die identifizierten B-F-Paare bzgl. der Kriterien für Sicherheitsschichten aus Abschnitt 3.2 geprüft, um so die Sicherheitsschichten des Beispiel-Bahnübergangs für die betrachtete Gefährdung zu identifizieren. Für die Überprüfung der Kriterien wird als Funktion eines B-F-Paars die Subfunktion aus Tabelle 9.5 verwendet.

Wirksamkeit

Wie in Abschnitt 6.6 beschrieben, wird zunächst die Wirksamkeit der B-F-Paare gegen die Gefährdung analysiert. Die Wirksamkeitsprüfung erfolgt für alle B-F-Paare aus Tabelle 9.5 – ungeachtet der Tatsache, dass die zugehörigen Strategien bereits auf ihre prinzipielle Wirksamkeit hin geprüft wurden. Auch wenn eine Strategie prinzipiell gegen eine Gefährdung wirken kann, darf daraus noch nicht gefolgert werden, dass alle ihre B-F-Paare gegen diese Gefährdung wirksam sind. Das Ergebnis der Prüfung wird zusammen mit dem Ergebnis der Prüfung der Unabhängigkeitskriterien in einer Tabelle (siehe Tabelle 9.6) dokumentiert.

Unabhängigkeit

Neben dem Wirksamkeitskriterium müssen die Sicherheitsschichten eines Systems auch den Unabhängigkeitskriterien genügen. Ein B-F-Paar ist unabhängig von allen anderen B-F-Paaren des betrachteten Systems (im Hinblick auf die betrachtete Gefährdung), wenn gilt (siehe auch Abschnitt 6.6.3):

- **a**) Die Funktion des B-F-Paars ist keine (echte) Teilfunktion eines anderen B-F-Paars.
- **b**) Die Barriere des B-F-Paars ist kein Teil einer Barriere eines anderen B-F-Paars.
- **c**) Es ist nicht die Funktion des B-F-Paars, ein anderes B-F-Paar zu aktivieren oder zu deaktivieren.
- **d**) Die Barriere des B-F-Paars ist nicht in der Lage, durch eine Fehlfunktion oder einen Ausfall eine Barriere eines anderen B-F-Paars zu deaktivieren oder in einer anderen Weise in ihrer Wirksamkeit zu beeinträchtigen.
- **e**) Die Barriere des B-F-Paars teilt kein technisches Betriebsmittel mit einer Barriere eines anderen B-F-Paars.

Für Barrieren, die mit Hilfe des Fehlerbaums identifiziert wurden (Schritt B), ist aufgrund der Methode sichergestellt, dass sie voneinander stochastisch unabhängig sind. Dadurch erfüllen diese Barrieren bereits die Kriterien **b**), **d**) und **e**). Dies gilt für alle Barrieren aus Tabelle 9.4. Diese Barrieren sind in den B-F-Paaren 1, 2, 3, 4, 5 und 8 enthalten. Allerdings kommen in diesen B-F-Paaren die Halbschranken doppelt vor: einmal in B-F-Paar 4 und einmal in B-F-Paar 8. Dies muss bei der Bewertung berücksichtigt werden. In Tabelle 9.6 geschieht dies durch das „id“ bei den Kriterien **b**), **d**) und **e**). Die Ergebnisse der Prüfung sind in Tabelle 9.6 dargestellt. Die Buchstaben V bis Z aus Tabelle 9.6 bezeichnen die Fußnoten für Erläuterungen:

Tabelle 9.6: Prüfung der Kriterien für Sicherheitsschichten für die Barriere-Funktions-Paare des Bahnübergangs-Beispiels

Barriere-Funktions-Paar				Kriterien						gehört
Funktion	**Subfunktion**	**Barriere**	**Nr.**	**Wirk.**	**a**	**b**	**c**	**d**	**e**	**zu**
Wege freigeben / verwehren	Züge physisch sichern / BÜ-Sicherung	PZB	1	+	+	+	+ (W)	+ (W)	+ (W)	
	Straßenverkehrsteilnehmer zum Warten vor dem BÜ auffordern	gelbe Lz	2	+	+ id (3, 4)	+	+	+	+ (X)	
		rote Lz	3	+	+ id (2, 4)	+	+	+	+ (X)	
		Halb-schranken	4	+	+ id (2, 3)	- id (8)	+	- id (8)	- id (8)	8
	Züge (Tf) visuell warnen	ÜS	5	+	+	+	+ (W)	+ (W)	+ (W)	
bewegliche Objekte detektieren	Straßenverkehrsteilnehmer detektieren, BÜ beobachten	Tf	6	+	+ (V)	M	+	M	n. a.	
	Aktivierung der Ankündigung des Zuges am BÜ	Einschalt-kontakt	7	-	+	+	- (2, 3, 4)	- (2, 3, 4)	+	2, 3, 4
Umgebung gestalten	Gefahrenbereich absperren, Straßenverkehrsteilnehmer physisch schützen, BÜ-Sicherung	Halb-schranken	8	+	+	- id (4)	+	- id (4)	- id (4)	4
informieren, warnen	Eisenbahnpersonal informieren: ÜS ankündigen	Rautentafel (Bü 2)	9	-	+	+	+	+	+	5
unterrichten, schulen	Eisenbahnpersonal unterrichten	Ausbildungs-betrieb, Berufs-schule	10	-	+	+	- (5, 6)	n. a. (Y)	n. a.	5, 6
Regeln aufschreiben und zugänglich machen	Regeln / Prozeduren für den Eisenbahnverkehr aufschreiben und zugänglich machen	Fahrdienst-vorschrift	11	-	+	+	- (10)	n. a. (Y)	n. a.	10
Verhalten üben	Erlerntes auffrischen	Sicherheits-training	12	-	+ (Z)	+	- (5, 6)	n. a. (Y)	n. a.	5, 6

V In Kombination mit der Handlung *Zug vor dem BÜ zum Stillstand bringen*.

W Es gibt durchaus eine Abhängigkeit zwischen der PZB, dem ÜS und den Elementen der BÜ-Sicherung: Schließen sich beispielsweise die Halbschranken nicht, so soll das ÜS Halt zeigen und die PZB den Zug bremsen. Ist die BÜ-Sicherung hingegen erfolgreich, dann soll das ÜS Fahrt zeigen und die PZB den Zug nicht bremsen. Diese Abhängigkeit beeinträchtigt jedoch nicht die Unabhängigkeit im Sinne der Sicherheitsschicht (SiS), denn es ist erwünscht, dass die PZB auf einen Ausfall der BÜ-Sicherung reagiert. Insbesondere führt z. B. ein Ausfall der Halbschranken nicht zu einem Ausfall der PZB (Kriterium **d**)).

X Die Unabhängigkeit ist hier stark von den Systemgrenzen abhängig. Würde man den Mast, an dem beide Lz angebracht sind, als Teil der Lz betrachten, so wären die roten und gelben Lz nicht unabhängig. Hier werden jedoch weder der Mast noch die Stromversorgung zu den Lz gerechnet.

Y Dieses B-F-Paar erbringt seine Funktion bereits vor dem eigentlichen Betrieb, hat also zum Zeitpunkt der eintretenden Gefährdung bereits gewirkt. Daher werden Fehlfunktionen während des Betriebs nicht betrachtet.

Z Wird nicht als Teil der Ausbildung angesehen.

Der Buchstabe **M** ohne Klammern in Tabelle 9.6 steht für den Sonderfall Mensch, siehe auch Abschnitt 3.2.7. Dies betrifft den Triebfahrzeugführer im B-F-Paar 6 bei den Kriterien **b**) und **d**). Diese Kriterien werden positiv bewertet, obwohl der Triebfahrzeugführer am betrachteten BÜ noch Teil weiterer Barrieren ist. Der Triebfahrzeugführer ist z. B. an der Barriere Überwachungssignal beteiligt, da er den Signalbegriff erkennen und entsprechend handeln muss. Tritt bei einer technischen Komponente ein Fehler bei der Erfüllung einer Funktion auf, wird davon ausgegangen, dass die technische Komponente auch ihre anderen Funktionen nicht mehr fehlerfrei erfüllen kann. Dies entspricht einem Totalausfall der Komponente. Da bei einem Menschen ein Fehler in der Regel nicht mit einem Totalausfall gleichzusetzen ist, müssen diese Unabhängigkeitskriterien hier nicht so streng ausgelegt werden wie bei technischen Komponenten. Daher werden die Kriterien **b**) und **d**) nicht mit + oder -, sondern mit M und damit als erfüllt bewertet.
Bzgl. der Schulungsmaßnahmen (Strategie 6) ist anzumerken, dass hier nach Belieben verfeinert und präzisiert werden kann. Das gilt insbesondere für das B-F-Paar 11. Liegt der Fokus vor allem auf dem technischen System, genügt ein allgemeiner Verweis auf die Fahrdienstvorschrift. Ist hingegen das Regelwerk selbst von Interesse, so können auch konkret einzelne Paragraphen genannt werden.

9.4.3 Ergebnis

Das Ergebnis dieses Schritts besteht aus der Tabelle, die die Ergebnisse der Prüfung der Kriterien für Sicherheitsschichten enthält (Tabelle 9.6), und der Liste mit Sicherheitsschichten für die Gefährdung „Zug befährt ungesicherten BÜ“:

I) Züge physisch sichern – PZB (B-F-Paar 1)
II) Straßenverkehrsteilnehmer zum Warten vor dem BÜ auffordern – gelbe Lichtzeichen (B-F-Paar 2)
III) Straßenverkehrsteilnehmer zum Warten vor dem BÜ auffordern – rote Lichtzeichen (B-F-Paar 3)
IV) Gefahrenbereich absperren, Straßenverkehrsteilnehmer physisch schützen (und Straßenverkehrsteilnehmer zum Warten vor dem BÜ auffordern) – Halbschranken (B-F-Paar 8 mit B-F-Paar 4)
V) Züge (Tf) visuell warnen – Überwachungssignal (B-F-Paar 5)
VI) Straßenverkehrsteilnehmer detektieren, BÜ beobachten – Triebfahrzeugführer (B-F-Paar 6)

Die Nummerierung I bis VI dient der eindeutigen Bezeichnung der Sicherheitsschichten und der Referenzierung in Abbildung 9.2, stellt aber keine Reihenfolge bzgl. des Wirkens dar (siehe auch

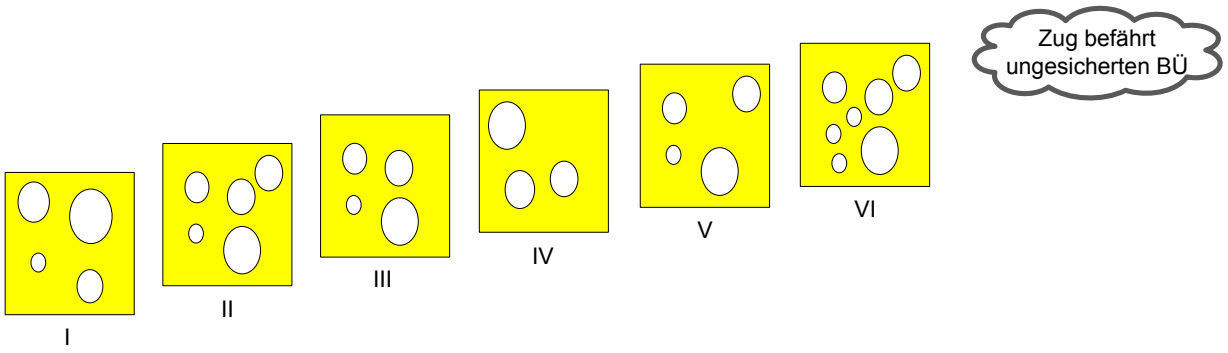

Abbildung 9.2: Identifizierte Sicherheitsschichten im Schweizer-Käse-Modell

Abschnitt 6.6.5). Im Vergleich zum Ergebnis aus Schritt C wurden aus den 12 B-F-Paaren aus Tabelle 9.5 die 6 oben genannten SiS identifiziert. Dabei entsprechen die 6 identifizierten SiS nicht den 6 B-F-Paaren, die ursprünglich in Tabelle 9.4 auf Basis der Barrieren im Fehlerbaum (Schritt B) identifiziert wurden. Jeder der Schritte der ISES-Methode bringt somit einen *erkennbaren Mehrwert* bei der Identifikation der SiS.
Zu den Sicherheitsschichten I bis VI wurden zudem weitere B-F-Paare identifiziert, die zu diesen SiS gehören, wie Tabelle 9.6 entnommen werden kann. Z. B. das B-F-Paar 7 (Aktivierung der Ankündigung des Zuges am BÜ – Einschaltkontakt). Der Einschaltkontakt ist eine Barriere, aber keine Sicherheitsschicht. Das B-F-Paar 7 gehört zu den B-F-Paaren 2, 3 und 4. Diese Zusammengehörigkeit ist bei einer späteren Betrachtung der Leistungsfähigkeit der Sicherheitsschichten von Bedeutung.

9.5 Veränderung des Beispiel-Bahnübergangs durch die Einführung von ETCS

In diesem Abschnitt wird das Vorgehen zum Austausch von Sicherheitsschichten (Abschnitt 7.6) auf den Beispiel-Bahnübergang aus Kapitel 8 angewendet. Dabei werden die in Schritt D der ISES-Methode identifizierten Sicherheitsschichten (Abschnitt 9.4.3) als Eingangsinformationen genutzt. Als Anlass für einen Austausch von Sicherheitsschichten dient in diesem Beispiel die Einführung des europäisch einheitlichen Zugsicherungssystems *European Train Control System (ETCS)*.

9.5.1 Situation

Die Europäische Union (EU) hat mit der Richtlinie 96/48/EG[4] [Eur96] die Einführung des europäisch einheitlichen Zugsicherungssystems ETCS auf den Weg gebracht. Im Zuge der Einführung von ETCS müssen unter anderem auf der Streckenseite Veränderungen vorgenommen werden. Die klassischen Zugsicherungssysteme werden langfristig entfernt und durch die neue Technik ersetzt.
Anmerkung: Nach dem derzeit gültigen Stand der Spezifikation von ETCS (Baseline 2) ist eine Umrüstung des Bahnübergangs (BÜ) aus Kapitel 8 ohne eine Änderung der Funktionsweise noch nicht möglich, da die Funktionalität von Bahnübergängen vom Typ ÜS noch nicht von dieser Baseline von ETCS abgedeckt wird. Dies ist erst ab der ETCS-Spezifikation *Baseline 3* möglich (derzeit noch nicht verbindlich). Für das Beispiel wird dazu die derzeit vorliegende Version für die ETCS-Spezifikation *Baseline 3*, insbesondere die System-Anforderungsspezifikation Subset-026 [ERA12], verwendet.

[4] Diese erste Interoperabilitätsrichtlinie ist inzwischen veraltet. Aktuell gültig ist die Richtlinie 2008/57/EG [Eur08] mit ihren Änderungen.

9.5.2 Veränderung

Ein Hersteller von Bahnübergangstechnik erhält von einem Eisenbahninfrastrukturbetreiber den Auftrag, den in Kapitel 8 beschriebenen Bahnübergang umzurüsten. Die Strecke, an der der Bahnübergang liegt, soll mit ETCS Level 1 ausgerüstet werden. Alle nationalen Zugbeeinflussungssysteme sollen entfernt werden. Die Signale sollen jedoch erhalten bleiben. Auch alle anderen Ausrüstungen des BÜ (Lichtzeichen, Halbschranken, ...) sollen unverändert bleiben.
Für den Auftragnehmer bedeutet dies, dass der 1000-Hz-Magnet der PZB als Teil des nationalen Zugbeeinflussungssystems entfernt werden soll. Stattdessen soll eine ETCS-Streckeneinrichtung eingebaut werden, die den Betrieb mit dem räumlich autark arbeitenden Bahnübergang mit Überwachungssignal unterstützt. Bei ETCS werden als Mittel für die punktförmige Übertragung von Information der Strecke an den Zug Eurobalisen (kurz: Balisen) verwendet. Diese Balisen können je nach Situation verschiedene Informationen übertragen. Für einen BÜ mit technischer Sicherung gibt es die Möglichkeit, Bahnübergangs-Informationen (in der Spezifikation *Packet Number 88: Level Crossing Information*) an den Zug zu übertragen. Diese Bahnübergangs-Informationen teilen mit, ob der BÜ gesichert ist und falls nicht, wird eine räumlich begrenzte Geschwindigkeitsbeschränkung (als sog. *Static Speed Restriction*) angeordnet. Zusätzlich zu der reduzierten Geschwindigkeit, mit der ein defekter, nicht gesicherter BÜ befahren werden darf, kann mit den Bahnübergangs-Informationen auch der Befehl, vor dem BÜ zu halten, übertragen werden.

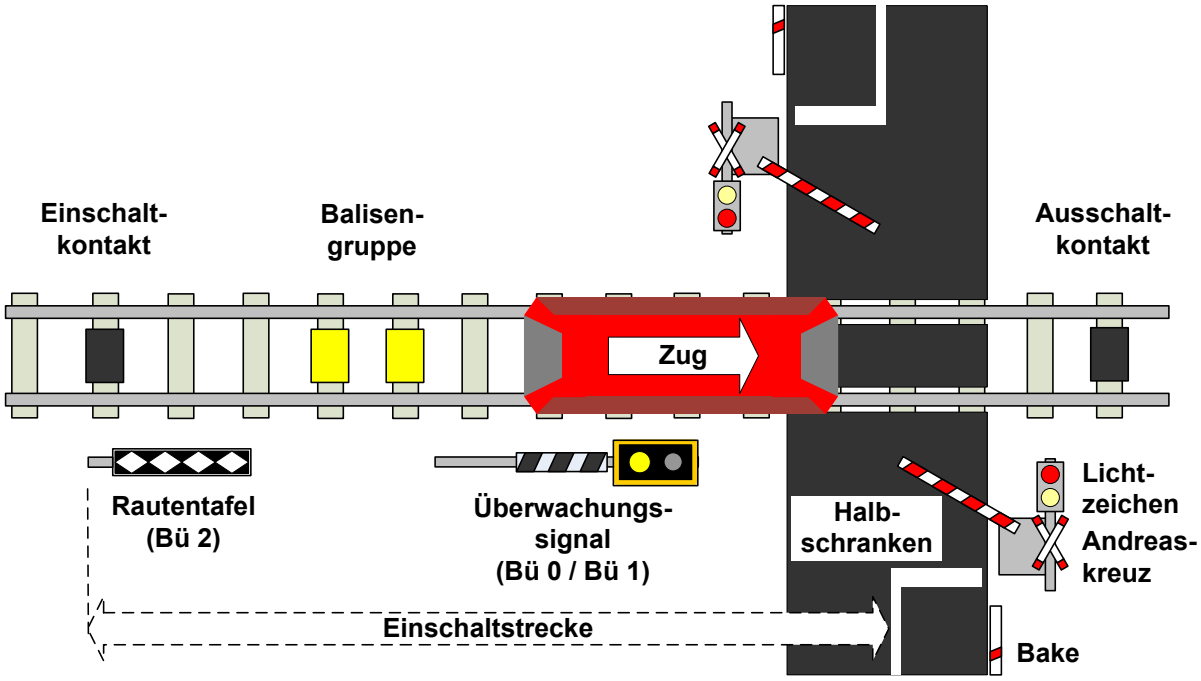

Abbildung 9.3: Beispiel-Bahnübergang mit ETCS

Anmerkung: Ein Überwachungssignal kann im ETCS Level 1 aus betrieblichen Gründen nicht wie ein Halt zeigendes Signal gesichert werden. Bei einem Halt zeigenden Signal wird dem Zug eine Fahrerlaubnis (*Movement Authority*) der Länge 0 m übergeben. In Level 1 sind Balisen (neben Radio Infill und Euroloop[5]) die einzige Möglichkeit, durch die die Streckenseite direkt Informationen an den Zug schicken kann (anders geht es nur noch über den Tf, per Sprachfunk, sofern vorhanden). Wird einem Zug eine Fahrerlaubnis (*Movement Authority*) der Länge 0 m übergeben, so kann er im Rahmen dieser Fahrerlaubnis nicht mehr weiter fahren. Daher kann er sich nicht dem BÜ nähern (um ihn z. B. manuell zu sichern) und auch keine weitere Balise überfahren, durch die er möglicherweise eine neue Fahrerlaubnis erhalten könnte. Der Ausweg aus dieser Situation bestünde darin, dass der Tf

[5]Radio Infill oder Infill über Euroloop, derzeit wird beides nur selten genutzt

manuell die technische Vollüberwachung des Zuges deaktiviert und den Zug stattdessen unter seiner eigenen persönlichen vollen Verantwortung (sog. *Staff Responsible Mode*) fährt, solange bis er wieder Informationen von der Streckenseite erhält (und das kann durchaus eine lange Strecke sein). Diese Prozedur ist aus betrieblichen Gründen nicht erwünscht, denn in dieser Rückfallebene besteht eine deutliche höhere Wahrscheinlichkeit für das Eintreten einer Gefährdung. Aus diesem Grund wurden die Bahnübergangs-Informationen spezifiziert. Mit diesen Bahnübergangs-Informationen bleibt der Zug ständig unter technischer Überwachung. Ein Wechsel in *Staff Responsible Mode* und damit ein Verlassen der technischen Sicherung ist nicht notwendig.
Um das Verhalten der PZB zu imitieren, wird an Stelle der PZB eine Balisengruppe[6] ins Gleis gelegt (siehe Abbildung 9.3), die die Bahnübergangs-Informationen in Abhängigkeit vom Status des BÜ überträgt. Im Falle eines ungesicherten BÜ ist es die Aufgabe der PZB, den Zug vor dem BÜ zum Halten zu bringen. Entsprechend wird die Balisengruppe so ausgelegt, dass sie den Befehl, vor dem BÜ zu halten, enthält.

9.5.3 Sicherheitsschichten vorher – nachher

Das prinzipielle Vorgehen für den Austausch von Sicherheitsschichten (SiS) ist in Abschnitt 7.6 beschrieben. Vor der Umrüstung besaß der Bahnübergang mit Überwachungssignal aus Kapitel 8 die folgenden Sicherheitsschichten (siehe Abschnitt 9.4.3):

I) Züge physisch sichern – PZB
II) Straßenverkehrsteilnehmer zum Warten vor dem BÜ auffordern – gelbe Lichtzeichen
III) Straßenverkehrsteilnehmer zum Warten vor dem BÜ auffordern – rote Lichtzeichen
IV) Gefahrenbereich absperren, Straßenverkehrsteilnehmer physisch schützen (und Straßenverkehrsteilnehmer zum Warten vor dem BÜ auffordern) – Halbschranken
V) Züge (Tf) visuell warnen – Überwachungssignal
VI) Straßenverkehrsteilnehmer detektieren, BÜ beobachten – Triebfahrzeugführer

Im Beispiel der Einführung von ETCS an einem Bahnübergang ist konkret die Sicherheitsschicht Nr. I aus dem Bahnübergangs-Beispiel betroffen. Ihre Barriere, die PZB, soll entfernt werden (streckenseitiger Anteil, der fahrzeugseitige Anteil muss als Folge davon angepasst werden). Damit fällt die gesamte SiS Nr. I weg. An ihrer Stelle wird eine andere SiS eingefügt, eine SiS I' (siehe Abbildung 9.4). Diese neue SiS besitzt die gleiche Funktion wie die alte SiS: „Züge physisch sichern", verwendet als Barriere jedoch keine PZB, sondern eine ETCS Balisengruppe.

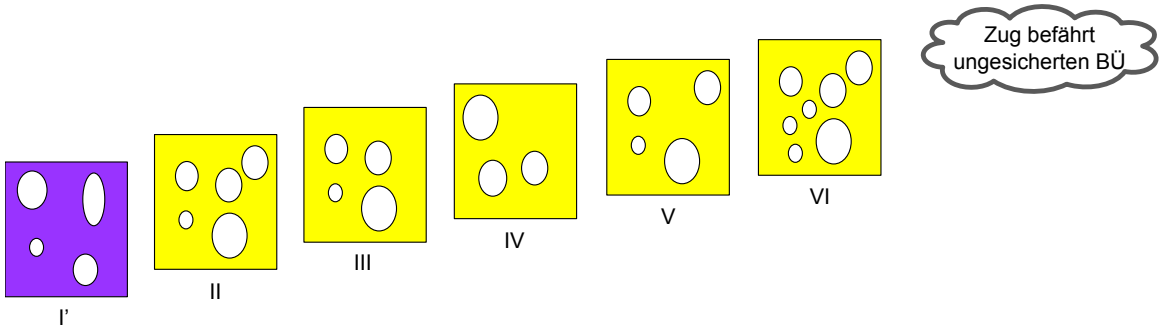

Abbildung 9.4: Sicherheitsschichten des Beispiel-Bahnübergangs mit ETCS

Mit dem ETCS-Mode *Limited Supervision*, der in der ETCS-Spezifikation *Baseline 3* enthalten ist, lässt sich das betriebliche Verhalten der PZB sehr gut nachbilden (siehe z. B. [MF10]). Für den

[6] Wichtige Informationen werden aus Gründen der Sicherheit nicht durch einzelne Balisen, sondern immer durch Balisengruppen mit zwei oder mehr Balisen übertragen.

Fall eines Bahnübergangs mit Überwachungssignal wird die neue ETCS-Spezifikation sogar noch weitere Möglichkeiten bieten (siehe [SL11]). Ist ein BÜ gestört, so muss der Zug gemäß betrieblichen Regeln am Halt zeigenden ÜS vorbeifahren. Dabei kann der Zug noch in vielen Punkten, mit Hilfe der Information der Balisengruppe, unter technischer Überwachung durch das ETCS-Fahrzeuggerät bleiben. Bei gleicher Verfügbarkeit kann durch die Nutzung dieser neuen Funktionen die Sicherheit der SiS nicht nur erhalten bleiben, sondern sogar noch weiter verbessert werden. Wichtig hierfür ist, dass die Unabhängigkeitskriterien überprüft werden. Wenn die Balisengruppe die Informationen über den Zustand des BÜ auf die gleiche Weise erhält wie die PZB, dann bleibt die Unabhängigkeit der anderen SiS erhalten. Die Balisengruppe erhält ihre Informationen von einer *Lineside Electronic Unit (LEU)*. Wenn die LEU ihre Informationen über den Zustand des BÜ dadurch gewinnt, dass sie den Signalbegriff des ÜS abgreift, dann ist die neue SiS I' nicht mehr unabhängig von der SiS V, die die Barriere ÜS enthält. In diesem Fall würden die SiS I' und V zu einer einzigen SiS zusammengefasst, und das System hätte nur noch fünf SiS. Die neue SiS wäre dann allerdings deutlich sicherer als die SiS I zuvor. Bleibt die Unabhängigkeit jedoch erhalten, bleibt auch die Anzahl der SiS gleich.

9.5.4 Sicherheitsnachweisführung

Der Hersteller, der den BÜ umrüstet, erhält vom Eisenbahninfrastrukturbetreiber zudem den Auftrag, alle notwendigen Schritte für eine behördliche Zulassung / Inbetriebnahmegenehmigung des BÜ vorzubereiten. Der Betreiber und die zulassende Behörde sind sehr daran interessiert, dass sich die Sicherheit des BÜ durch die Einführung des neuen Zugsicherungssystems, also durch den Umbau, nicht verschlechtert. Der BÜ soll mindestens genauso sicher sein wie vor dem Umbau. Um dies zu zeigen, kann ein Sicherheitsnachweis mit dem Risikoakzeptanzkriterium *Mindestens Gleiche Sicherheit (MGS)* durchgeführt werden. Schwierig wird dieser Nachweis dann, wenn der Grad der Sicherheit bzw. des Risikos für den alten BÜ nicht bekannt ist. Viele Systeme wurden gebaut und in Betrieb genommen, bevor Vorschriften und Normen die Angabe von Gefährdungsraten erforderten. Wenn für den umgebauten BÜ eine Gefährdungsrate (HR) berechnet wird, kann diese nicht mit der HR des alten BÜ verglichen werden, weil letztere nie bestimmt wurde. Sie nachträglich zu berechnen ist ein hoher Aufwand, evtl. sogar unmöglich, wenn die Daten für die alten, möglicherweise längst abgekündigten Bauteile nicht mehr zu bekommen sind. Zudem ergibt sich kaum ein Vorteil aus einer derartigen Berechnung. Schließlich wird das System gerade verändert, sodass eine HR berechnet würde, die auf das System anschließend mit ziemlicher Sicherheit nicht mehr zutrifft. Dieses Problem kann dadurch reduziert werden, dass der unveränderte Teil aus der Betrachtung ausgeklammert und ein Nachweis gleicher Sicherheit nur für die veränderte SiS (und ggf. andere veränderte Bauteile) durchgeführt wird. Bei dieser Vorgehensweise muss in jedem Fall die Rückwirkungsfreiheit des betrachteten Teils des Systems auf den nicht betrachteten Teil sichergestellt sein.

Statt des gesamten Systems nur zwei Sicherheitsschichten zu vergleichen, reduziert den Aufwand deutlich. Es muss nur ein klar abgegrenzter Bereich untersucht werden. Möglicherweise kann für diesen abgegrenzten Bereich sogar eine Berechnung der HR der alten SiS zum Vergleich stattfinden. Aufgrund der Unabhängigkeitsanforderungen an Sicherheitsschichten reduziert sich auch der Aufwand für den Nachweis der Rückwirkungsfreiheit, auch wenn auf eine CCF-Analyse nicht verzichtet werden kann.

So wie der Aufwand für die Sicherheitsnachweisführung, so reduziert sich auch der Aufwand für die nachfolgende Prüfung und Begutachtung. Durch die klare Struktur und dadurch, dass der zu betrachtende Systembereich klar abgegrenzt ist, reduzieren sich sowohl Aufwand als auch Kosten, denn externe Begutachtungen verursachen höhere Kosten als herstellerinterne Vorarbeiten. Zudem reduziert sich der Zeitbedarf für das Projekt insgesamt: Das System kann früher zugelassen und in Betrieb genommen werden, siehe auch Abschnitt 3.5.

9.5.5 Fazit

Am Beispiel der Änderung eines bestehenden Eisenbahnsystems durch die Einführung von ETCS wurde dargestellt, wie ein Austausch von Sicherheitsschichten gemäß dem in Abschnitt 7.6 vorgestellten Verfahren durchgeführt wird. Änderungen an bestehenden Systemen sind in Europa keine Ausnahme, sondern vielmehr die Regel, da Europa bereits über ein großes Eisenbahnsystem verfügt. Daher kommt der Bewertung der Sicherheit bei Änderungen eine große Bedeutung zu. Gleichsam ist die Dokumentation zur Nachweisführung oft ungünstig aufbereitet und nicht nach Sicherheitsgesichtspunkten strukturiert, was bei der Begutachtung und Zulassung zu zusätzlichen Kosten führt. Die Kosten für eine Änderungszulassung können dabei so groß werden, dass kleinere Änderungen gar nicht durchgeführt werden, da man den Aufwand und die Kosten scheut.
Am Beispiel der Einführung von ETCS wurde aufgezeigt, welcher Nutzen aus der Anwendung des Konzepts der Sicherheitsschichten gewonnen werden kann. Das Konzept der Sicherheitsschichten ermöglicht ein formalisiertes, deutlich strukturiertes Vorgehen, das Aufwand, Zeit und Kosten sparen kann. Die technischen Änderungen werden in Form betroffener Sicherheitsschichten beschrieben, sodass der Bereich, der von den Änderungen betroffen ist, klar abgegrenzt werden kann. Die Auswirkungen auf die Sicherheit werden direkt deutlich, wodurch die Arbeit von Gutachtern und zulassenden Behörden erleichtert wird. Die Unabhängigkeitskriterien der Sicherheitsschichten erleichtern die Sicherheitsnachweisführung zusätzlich.

10 Validierung und weiterführende Betrachtungen

Validierung bezeichnet die „Bestätigung durch Überprüfung und objektiven Nachweis, dass die besonderen Anforderungen für einen spezifischen, bestimmungsgemäßen Gebrauch erfüllt wurden“ [DIN00, 3.44]. Im Bereich der Eisenbahn ist die Validierung von großer Bedeutung für die Entwicklung von Systemen, sodass ihr eine eigene Phase im Lebenszyklus des Systems nach DIN EN 50126-1 [DIN00] gewidmet wird. Aus diesem Grund soll die Validierung in diesem Kapitel als eigenständige Aufgabe zusammenfassend bearbeitet werden. Im Rahmen der Validierung wird geprüft, ob das „richtige Produkt“ erstellt wird [B06]. Das Produkt im Sinne der vorliegenden Arbeit besteht aus dem Begriff *Sicherheitsschicht* und der *ISES-Methode*. „Richtig“ ist dieses Produkt dann, wenn es die Anforderungen aus den Abschnitten 3.1 und 5.1 erfüllt.
Die Überprüfung der Erfüllung von festgelegten Anforderungen wird auch als Verifikation bezeichnet [DIN00]. Im Gegensatz zur Validierung wird der „bestimmungsgemäße Gebrauch“ dabei nicht berücksichtigt. Stattdessen erfolgt die Verifikation in der Regel gegen eine Spezifikation. Die in den Abschnitten 3.1 und 5.1 definierten Anforderungen beinhalten jedoch nicht nur konkrete Anforderungen, wie z. B. dass der Begriff Sicherheitsschicht technische Aspekte umfassen und die Methode einen deduktiven Anteil haben soll. Sie beinhalten auch „Anforderungen für einen spezifischen, bestimmungsgemäßen Gebrauch“ [DIN00], z. B. die Anforderung, dass die Methode für den Bahnbereich anwendbar sein soll. Daher erfolgt die Überprüfung der Erfüllung der Anforderungen im Folgenden unter dem Begriff *Validierung*.
Zunächst wird die Erfüllung der Anforderungen an den Begriff Sicherheitsschicht und die ISES-Methode geprüft. Anschließend wird zusammenfassend die Erfüllung der „Anforderungen für einen spezifischen, bestimmungsgemäßen Gebrauch“ [DIN00] bewertet. Ein weiterführende Betrachtung zur Verbindung zwischen Sicherheitsschichten und Unfallanalysen rundet die Bewertung von Begriff und Methode ab.

10.1 Erfüllung der Anforderungen an Sicherheitsschichten und an die ISES-Methode

Im Rahmen dieser Arbeit wurden Anforderungen an Sicherheitsschichten (Abschnitt 3.1) und Anforderungen an eine gesuchte Methode (Abschnitt 5.1) definiert. Im Folgenden soll geprüft werden, ob der Begriff der Sicherheitsschicht und die ISES-Methode diesen Anforderungen genügen.

10.1.1 Erfüllung der Anforderungen an Sicherheitsschichten

In Abschnitt 3.1 wurden 14 Anforderungen an Sicherheitsschichten aufgestellt: S-1 bis S-14. In Tabelle 10.1 wird betrachtet, ob die gestellten Anforderungen durch die Sicherheitsschichten, wie sie in Abschnitt 3.2 definiert wurden, erfüllt werden.

Tabelle 10.1: Erfüllung der Anforderungen an Sicherheitsschichten aus Abschnitt 3.1

Nr.	Anforderung	Kommentar	Siehe Abschnitt	Erfüllung
S-1	Sicherheitsschichten sollen Bausteine in einem Baukasten sein, um ein Portfolio bilden zu können, wie in [SP07] gefordert.	Sicherheitsschichten sind eigenständige, klar abgegrenzte, voneinander unabhängige Systemelemente. Dadurch können sie wie **Bausteine** in einem Baukasten verwendet werden. Somit ist es möglich, ein **Portfolio** aus Sicherheitsschichten zu bilden, wie in [SP07] gefordert.	3.2.5	+
S-2	Sicherheitsschichten sollen einen modularen und flexiblen Aufbau von Sicherheitssystemen ermöglichen, wie in [PSM07] gefordert.	Das Konzept der Sicherheitsschichten ermöglicht es, die Sicherheitsmaßnahmen eines Systems **modular** zu betrachten. Die „Module“ entsprechen dabei den Sicherheitsschichten. Zusammen mit den Anforderungen S-9 und S-10 ermöglicht das Konzept einen **flexiblen** Aufbau von Sicherheitssystemen. Damit wird die Anforderung aus [PSM07] nach einem modularen Aufbau erfüllt.	3.2.5	+
S-3	Sicherheitsschichten sollen für Sicherheitsnachweise verwendet werden können, damit die Kenntnis der Sicherheitsschichten eines Systems auch Vorteile bei der Zulassung mit sich bringt.	Sicherheitsschichten können für **Sicherheitsnachweise** verwendet werden, um die im System vorhandenen unabhängigen und wirksamen Sicherheitsmaßnahmen gefährdungsbezogen zu beschreiben. Bei einer Delta-Betrachtung aufgrund einer Änderung am System kann das Modell der Sicherheitsschichten zu einer Reduzierung des Aufwands bei der Erstellung des (Delta-)Sicherheitsnachweises führen.	3.5, 7.3, 7.5, 9.5.4	+

Tabelle 10.1: Erfüllung der Anforderungen an Sicherheitsschichten (Fortsetzung)

Nr.	Anforderung	Kommentar	Siehe Abschnitt	Erfüllung
S-4	Sicherheitsschichten sollen Raum für Innovationen und andere Lösungen geben, um eine beständige Weiterentwicklung der Sicherheitssysteme zu ermöglichen und Kosten zu sparen.	Sicherheitsschichten bieten Raum für **Innovationen** und neue Lösungen, da sie eine Möglichkeit bieten, Änderungen am System aufwandsarm zu bewerten und verschiedene Lösungen miteinander zu vergleichen.	7.6, 9.5	+
S-5	Der Begriff Sicherheitsschicht soll klar definiert sein.	Der Begriff Sicherheitsschicht und seine Teilbegriffe wurden im Rahmen der vorliegenden Arbeit **klar definiert**. Es wurden zudem klare Kriterien aufgestellt, um zu entscheiden, ob ein Barriere-Funktions-Paar eine Sicherheitsschicht ist.	3.2	+
S-6	Der Begriff Sicherheitsschicht soll funktionale Aspekte umfassen, um den funktionalen Ansatz der CENELEC-Normen zu berücksichtigen.	Der Begriff Sicherheitsschicht umfasst **funktionale Aspekte** dadurch, dass eine Sicherheitsschicht ein Barriere-Funktions-Paar ist, das bestimmte Kriterien erfüllt. Dadurch wird der funktionale Ansatz der CENELEC-Normen unterstützt.	3.2	+
S-7	Der Begriff Sicherheitsschicht soll technische Aspekte umfassen. Systementwickler aus dem Eisenbahnbereich denken bevorzugt in Form von technischen Komponenten. Eine rein funktionale Betrachtungsweise von Sicherheitsschichten wäre daher nicht ausreichend. Außerdem ist es die Technik, die letztendlich gebaut und zugelassen werden soll.	Der Begriff Sicherheitsschicht umfasst **technische Aspekte** durch die enthaltene Barriere. Beinhaltet eine Sicherheitsschicht ein technisches System, so ist dies Bestandteil der Barriere der Sicherheitsschicht. Allerdings enthält nicht jede Sicherheitsschicht zwangsläufig technische Elemente. Ein Sonderfall sind Sicherheitsschichten mit der Barriere Mensch: In der Regel nutzt der Mensch bei der Ausübung seiner Sicherheitsfunktion technische Systeme, wie z. B. Tachometer oder Bremshebel. Da die eigentliche Funktion vom Menschen erbracht wird und die	3.2	+

Tabelle 10.1: Erfüllung der Anforderungen an Sicherheitsschichten (Fortsetzung)

Nr.	Anforderung	Kommentar	Siehe Abschnitt	Erfüllung
		technischen Systeme hierbei nur Hilfsmittel sind, werden die technischen Elemente bei der Benennung der entsprechenden Sicherheitsschicht vernachlässigt.		
S-8	Der Begriff Sicherheitsschicht soll Organisatorisches, wie z. B. Regeln, und Menschen umfassen. Es wird ein ganzheitlicher Ansatz benötigt. Dies wird auch von den CENELEC-Normen gefordert.	Der Begriff Sicherheitsschicht umfasst **Organisatorisches**, wie z. B. Regeln, und auch den **Menschen** als Barriere.	3.2.2, 3.4, 9.3	+
S-9	Sicherheitsschichten sollen so gestaltet sein, dass das Entfernen einer Sicherheitsschicht die anderen noch verbleibenden Sicherheitsschichten nicht beeinflusst.	Wird eine **Sicherheitsschicht** aus dem System **entfernt**, beeinflusst dies die verbleibenden Sicherheitsschichten nicht. Dies ist durch die Unabhängigkeitskriterien sichergestellt.	3.2.5, 7.6	+
S-10	Sicherheitsschichten sollen so gestaltet sein, dass eine Sicherheitsschicht gegen eine andere ausgetauscht werden kann, ohne dass das Gesamtsystem einer komplett neuen, aufwändigen Bewertung unterzogen werden muss.	Wird eine Sicherheitsschicht aus dem System entfernt und durch eine andere ersetzt / **ausgetauscht**, dann ist der **Aufwand für eine Bewertung** des geänderten Systems geringer als der Aufwand für eine komplette Neubewertung.	7.5, 7.6, 9.5	+
S-11	Der Begriff Sicherheitsschicht soll Aspekte zur Unabhängigkeit enthalten. Unabhängigkeit ist beim Erreichen einer angemessenen Sicherheit im Eisenbahnbereich ein bedeutendes Prinzip. Jeder Sicherheitsnachweis muss Auskunft über die Unabhängigkeit der Einheiten des Systems geben.	Der Begriff Sicherheitsschicht beinhaltet **Aspekte zur Unabhängigkeit**. Jede Sicherheitsschicht erfüllt die fünf Unabhängigkeitskriterien **a**) bis **e**).	3.2.5	+

Tabelle 10.1: Erfüllung der Anforderungen an Sicherheitsschichten (Fortsetzung)

Nr.	Anforderung	Kommentar	Siehe Abschnitt	Erfüllung
S-12	Der Begriff Sicherheitsschicht soll auf Gefährdungen bezogen sein. Dies harmoniert mit dem Ansatz der CENELEC-Normen, bei denen Maßnahmen zur Risikominderung im Hinblick auf Gefährdungen definiert und dokumentiert werden, u. a. im sogenannten Gefahrenprotokoll (Hazard Log), siehe [DIN00].	Der Begriff Sicherheitsschicht ist **bezogen auf Gefährdungen**. Dies wird auch in der Gefährdungs-Sicherheitsschichten-Matrix (Tabelle 7.1) deutlich.	3.2, 7.3	+
S-13	Eine Sicherheitsschicht braucht keine Mindestanforderungen bezüglich der Risikoreduktion zu erfüllen. Sie muss das Risiko nicht um einen bestimmten Mindestfaktor reduzieren (im Gegensatz zu anderen Konzepten, vergleiche Abschnitt 2.3.3). Kleine Beiträge zur Sicherheit sind ebenfalls nutzbringend.	Es werden keine Anforderungen an Sicherheitsschichten bzgl. der **Höhe ihrer Risikoreduktion** gestellt. Maßnahmen zur Verbesserung der Sicherheit werden nicht aus dem Konzept der Sicherheitsschichten ausgeschlossen, wenn sie das Risiko nur wenig senken. Jeder Beitrag zur Verbesserung der Sicherheit kann in das Modell der Sicherheitsschichten aufgenommen werden, wenn er die Kriterien für Sicherheitsschichten erfüllt.	3.2	+
S-14	Ein Modell der Sicherheitsschichten braucht keine festgelegte Reihenfolge zu beinhalten (im Gegensatz zu anderen Konzepten, vergleiche z. B. Abschnitt 4.3). Es ist unwichtig, in welcher Reihenfolge Sicherheitsschichten wirken, solange sie der Sicherheit des Systems dienen.	Das Modell der Sicherheitsschichten ist **unabhängig von der Reihenfolge** der Sicherheitsschichten im Modell. Es unterscheidet weder nach der räumlichen noch zeitlichen Wirkung der Sicherheitsschichten. Auf diese Weise wird das Modell einfach gehalten.	3.3.2	+

10.1.2 Erfüllung der Anforderungen an die ISES-Methode

In Abschnitt 5.1 wurden 12 Anforderungen an die gesuchte Methode aufgestellt: M-1 bis M-12. In Tabelle 10.2 wird betrachtet, ob die gestellten Anforderungen durch die ISES-Methode aus Kapitel 6 erfüllt werden.

Tabelle 10.2: Erfüllung der Anforderungen an die ISES-Methode aus Abschnitt 5.1

Nr.	Anforderung	Kommentar	Siehe Abschnitt	Erfüllung
M-1	Die Methode soll Sicherheitsmaßnahmen bzw. Sicherheitsschichten identifizieren.	Die ISES-Methode **identifiziert** die **Sicherheitsschichten** eines Systems. Als Teil davon identifiziert sie auch die zugehörigen **Sicherheitsmaßnahmen** in Form von Sicherheitsbarrieren und -funktionen.	6	+
M-2	Die Methode soll eine Basis für eine quantitative Bewertung der Sicherheitsmaßnahmen bzw. Sicherheitsschichten bereitstellen, um so die Anforderungen nach einer quantitativen Risikobetrachtung (Gefährdungsraten) der DIN EN 50129 [DIN03] erfüllen zu können.	Die ISES-Methode bewertet die identifizierten Sicherheitsschichten nicht. Jedoch stellt sie für eine nachfolgende **quantitative Bewertung** eine gute **Basis** bereit. Sicherheitsschichten werden bezogen auf Top-Level-Gefährdungen identifiziert. Für diese Gefährdungen werden in der Regel in einer Sicherheitsanforderungsspezifikation tolerierbare Gefährdungsraten (THRs) vorgegeben. Im Rahmen der Sicherheitsnachweisführung nach DIN EN 50129 [DIN03] muss die Einhaltung dieser THRs belegt werden. Durch die Unabhängigkeitskriterien, die von den Sicherheitsschichten erfüllt werden, wird die Quantifizierung erleichtert, da die Unabhängigkeit die Berechnung der Eintretenswahrscheinlichkeiten vereinfacht.	7.5	+
M-3	Die Methode soll für den Bahnbereich anwendbar sein.	Die ISES-Methode ist für den **Bahnbereich anwendbar**. Dies wurde anhand des Beispiels eines Bahnübergangs gezeigt.	9	+

Tabelle 10.2: Erfüllung der Anforderungen an die ISES-Methode (Fortsetzung)

Nr.	Anforderung	Kommentar	Siehe Abschnitt	Erfüllung
M-4	Die Methode soll geeignet sein, um ein generisches Modell der Sicherheitsschichten des Systems zu erzeugen (nicht nur ein anlagenspezifisches).	Die ISES-Methode lässt sich so anwenden, dass sich die Ergebnisse auf einem angemessen **generischen** Niveau befinden: Konkret genug, um den typischen eisenbahntechnischen Komponenten zu entsprechen (z. B. Zugbeeinflussung oder Schranken), aber nicht so anlagenspezifisch, dass die Aussagen nur für ein einziges System Gültigkeit haben. Z. B. lassen sich die Ergebnisse der Analyse des Bahnübergangs-Beispiels auf andere Bahnübergänge vom Typ ÜS übertragen. Die dort verwendete Analyseebene mit Halbschranken und Lichtzeichen ist weder hersteller- noch ortsspezifisch und damit nicht auf einen einzigen, bestimmten Bahnübergang beschränkt.	9	+
M-5	Die Ergebnisse der Methode sollen für die Sicherheitsnachweisführung weiterzuverwenden sein. Insbesondere ist hier der Abschnitt 3 (Ausfallauswirkungen) des technischen Sicherheitsberichts gemäß DIN EN 50129 [DIN03] zu berücksichtigen.	Die Ergebnisse der ISES-Methode können für die **Sicherheitsnachweisführung** verwendet werden. Dies betrifft in erster Linie die identifizierten Sicherheitsschichten und die Aussagen zur Unabhängigkeit, die für Abschnitt 3 (Ausfallauswirkungen) des Technischen Sicherheitsberichts gemäß DIN EN 50129 [DIN03] verwendet werden können. Auch die identifizierten, nicht unabhängigen Barriere-Funktions-Paare, können für die Nachweisführung weiterverwendet werden, denn sie geben wichtige Hinweise auf Abhängigkeiten innerhalb des Systems und die Leistungsfähigkeit der Sicherheitsschichten. Der Fehlerbaum, der im	3.5, 7.3, 7.5, 7.6, 9.5.4	+

Tabelle 10.2: Erfüllung der Anforderungen an die ISES-Methode (Fortsetzung)

Nr.	Anforderung	Kommentar	Siehe Abschnitt	Erfüllung
		Rahmen der ISES-Methode verwendet wird, kann ebenfalls im Rahmen der Sicherheitsnachweisführung weiter verwendet werden. Die genutzte Fehlerbaumanalyse (FTA) muss in der Regel jedoch um eine quantitative Auswertung erweitert werden. Einen besonderen Vorteil bietet die ISES-Methode bei der Sicherheitsnachweisführung von Systemänderungen.		
M-6	Die Methode soll alle Arten von Systemelementen behandeln können. Sie soll für technische Systeme geeignet sein, aber auch Raum für menschliche Einflüsse und Handlungen bieten sowie organisatorische Aspekte zulassen.	Die ISES-Methode identifiziert Sicherheitsschichten. Da der Begriff Sicherheitsschicht sowohl **technische** als auch **organisatorische** und **menschliche Aspekte** beinhaltet, beinhaltet die ISES-Methode diese auch. Durch die Nutzung von Checklisten wird der Fokus der Analyse, der sich klassischerweise auf die Technik konzentriert, zudem in Richtung organisatorischer und menschlicher Aspekte gelenkt. Dass die ISES-Methode zur Analyse eines technischen Systems geeignet ist und dabei auch menschliche Handlungen und Organisatorisches berücksichtigt, wurde anhand des Bahnübergangs-Beispiels gezeigt.	3.2, 9	+
M-7	Die Methode soll möglichst leicht zu erlernen sein, oder aber auf einer (evtl. schwierigen) Standard-Methode aus dem Eisenbahnbereich aufsetzen.	Der Aufwand, um die ISES-Methode zu *erlernen*, ist durchschnittlich, sie basiert jedoch auf einer **Standard-Methode** aus dem Eisenbahnbereich, der FTA. Durch die Arbeit mit Checklisten wird die Anwendung der ISES-Methode erleichtert. Die Prüfung der	6.3, 6.6.6, 9	+

Tabelle 10.2: Erfüllung der Anforderungen an die ISES-Methode (Fortsetzung)

Nr.	Anforderung	Kommentar	Siehe Abschnitt	Erfüllung
		Kriterien für Sicherheitsschichten (Schritt D) ist ein relativ schwieriger Schritt innerhalb der ISES-Methode, in dem der Analyst jedoch durch klare Kriterien geleitet wird. Um das Erlernen der ISES-Methode zu erleichtern, wurde ein ausführliches Beispiel dargestellt.		
M-8	Die Ergebnisse der Methode sollen in Form eines Modells graphisch darstellbar sein.	Die Ergebnisse der ISES-Methode können durch das Schweizer-Käse-Modell **graphisch dargestellt** werden.	4.12, 7.2	+
M-9	Die Methode soll präventiv, d. h. bereits vor einem Unfall, anwendbar sein.	Die ISES-Methode ist **präventiv anwendbar**. Sie kann bereits im Entwurfsstadium eingesetzt werden.	7.1	+
M-10	Die Methode soll Fehler- / Ausfallkombinationen berücksichtigen, denn 1-Fehler-Sicherheit ist in vielen Teilbereichen des Eisenbahnsystems bereits Standard.	Die ISES-Methode berücksichtigt **Fehler- und Ausfallkombinationen**, indem sie die Sicherheitsmaßnahmen eines Systems in mehrere Sicherheitsschichten untergliedert, die alle versagen müssen, damit eine Gefährdung eintritt.	6	+
M-11	Die Methode soll einen deduktiven Anteil haben, um den Anforderungen der DIN EN 50129 [DIN03] bzgl. der Betrachtung von Ausfällen nachzukommen.	Die ISES-Methode hat einen **deduktiven Anteil**, da sie eine deduktive Methode, die Fehlerbaumanalyse, beinhaltet.	5.10, 6.3	+
M-12	Die Methode soll einen induktiven Anteil haben, um die deduktive Analyse gemäß den Empfehlungen der DIN EN 50129 [DIN03] zu unterstützen.	Die ISES-Methode hat einen **induktiven Anteil**, da sie eine induktive Methode, die Barriereanalyse, nutzt.	5.10, 6.5	+

10.1.3 Fazit

Wie in den Tabellen 10.1 und 10.2 dargestellt, erfüllen sowohl der Begriff Sicherheitsschicht als auch die ISES-Methode alle an sie gestellten Anforderungen. Ihre *Anwendbarkeit* im Eisenbahnbereich wurde durch das Beispiel des Bahnübergangs aus Kapitel 9 demonstriert. Der *Nutzen* des Modells

der Sicherheitsschichten wurde insbesondere für den Bereich der Änderung von bestehenden Systemen anhand der Einführung von ETCS am Beispiel-Bahnübergang dargelegt (Abschnitt 9.5). Als Ergebnis der Validierung kann festgehalten werden, dass alle Anforderungen für einen spezifischen, bestimmungsgemäßen Gebrauch von Begriff und Methode erfüllt sind.

10.2 Verbindung zwischen Sicherheitsschichten und Unfallanalysen

Als ergänzende Betrachtung wird in diesem Abschnitt untersucht, wie sich das Modell der Sicherheitsschichten in bestehende Konzepte aus dem Bereich der Unfallanalyse einfügt. Der Zusammenhang zwischen dem Modell der Sicherheitsschichten und Unfallanalysen ist von Bedeutung, da nach Unfällen häufig ein großes Interesse besteht, das betroffene System zu verändern, um es sicherer zu gestalten. Um diesen Zusammenhang zu erläutern, wird im Folgenden ein Beinahe-Unfall an einem Bahnübergang analysiert. Das Ergebnis dieser Analyse wird dem Modell der Sicherheitsschichten des Beispiel-Bahnübergangs aus Kapitel 9 gegenübergestellt.

10.2.1 Unfallanalysen

Es gibt zwei grundsätzliche Arten von Analysen im Bereich der Sicherheit: *Präventive Analysen* und *Unfallanalysen*. Erstere dienen dazu, die Sicherheit eines Systems und das verbleibende Risiko für seine Benutzer einzuschätzen, bevor es zu einem Unfall kommt. In der Regel werden diese Analysen bereits vor der Inbetriebnahme des Systems durchgeführt und sind Grundlage für die Inbetriebnahmegenehmigung. Die Zweite Art der Analyse, die Unfallanalyse, dient dazu, nach dem Eintreten eines Unfalls die Ursachen zu finden. Das Interesse an den Ursachen von Unfällen hat zwei Gründe: zum einen die Klärung der Schuldfrage (z. B. gerichtlich oder für Versicherungsfragen), zum anderen das Lernen aus Fehlern, d. h. das Ableiten von Maßnahmen zur Verbesserung der Sicherheit, um eine Wiederholung des Unfalls zu vermeiden.

Mit beiden Arten von Analysen wird das gleiche System analysiert. Beide Male liegt der Fokus der Analyse auf der Sicherheit. Daher gibt es eine enge Verbindung zwischen diesen beiden Arten von Analysen. Besonders ist das daran zu erkennen, dass einige Methoden sowohl für präventive als auch für Unfallanalysen verwendet werden können, wie z. B. die Sicherheitsfunktionsanalyse (SFA) oder Barriereanalyse (BA) (siehe Abschnitte 5.4 und 5.5).

Die in Kapitel 6 vorgestellte ISES-Methode dient der *präventiven Analyse*. Sie identifiziert Sicherheitsschichten, die wiederum Barrieren enthalten. Viele Methoden zur Unfallanalyse verwenden das Konzept von Barrieren, um darzulegen, wie es zu einem Unfall kommen konnte. Sie fragen danach, welche Barrieren versagt haben und was getan werden muss, um sie zu stärken oder zu ergänzen, um eine Wiederholung des Unfalls zu vermeiden.

Verwendet man das Schweizer-Käse-Modell (SCM) als gedankliches Modell, dann müssen alle Barrieren / alle Sicherheitsschichten durchbrochen werden, damit es zu einem Unfall kommen kann. Die Ergebnisse einer Unfallanalyse beschreiben also, welchen Pfad durch alle Sicherheitsschichten hindurch der Unfallverlauf genommen hat.

Auch wenn eine Unfallanalysemethode das Konzept der Barrieren nicht explizit verwendet, so muss doch jedes wichtige Ergebnis einer guten Unfallanalyse eine Entsprechung in den Sicherheitsschichten haben. Wurde mit der ISES-Methode ein Modell der Sicherheitsschichten eines Systems aufgestellt, dann kann eine Verbindung zwischen den Ergebnissen einer Unfallanalyse und den identifizierten Sicherheitsschichten für das betroffene System hergestellt werden.

10.2.2 Analyse eines Beinahe-Unfalls am Bahnübergang Wupperweg

Um den Zusammenhang zwischen dem Modell der Sicherheitsschichten und den Ergebnissen einer Unfallanalyse zu zeigen, wird ein Beinahe-Unfall mit Hilfe einer Unfallanalysemethode untersucht. Dieser Beinahe-Unfall ereignete sich am 4.11.2010 an einem Bahnübergang in Köln. Der dortige Bahnübergang entspricht nicht ganz dem Bahnübergang aus Kapitel 8, ist diesem aber ähnlich. Als Analysemethode wird, wie in [SP07, PSM07, SP08] vorgeschlagen, die Why-Because-Analyse (WBA) (Abschnitt 5.3) verwendet.
Am 4.11.2010 fuhr eine Regionalbahn über einen Bahnübergang auf dem Wupperweg in Köln. Der Bahnübergang war mit einer technischen Bahnübergangssicherungsanlage ausgerüstet, die rote Blinklichter und Halbschranken umfasst. Augenzeugen berichteten, dass sich die Halbschranken des Bahnübergangs trotz des herannahenden Zuges nicht geschlossen hatten [Taa10]. Ein LKW-Fahrer hatte den Zug bemerkt und konnte einen Unfall gerade noch verhindern.
Für eine WBA wird in der Regel ein Unfalluntersuchungsbericht als Basis verwendet. Da für diesen Beinahe-Unfall bislang kein offizieller Unfalluntersuchungsbericht vorliegt, werden als Quellen Zeitungsartikel [Taa10, Die10b, Die10a, Sti10][1] und ein Satellitenbild (Abbildung C.2, Anhang C) verwendet. Mit Hilfe dieser Quellen wurde eine ungefähre Systembeschreibung des Bahnübergangs erstellt. Dabei wurden Lücken in der Dokumentation durch sinnvolle Annahmen gefüllt. Da an dieser Stelle eine Unfallanalyse nur zu dem Zweck durchgeführt wird, die Verbindung zwischen Unfallanalysen und Sicherheitsschichten darzustellen, ist dieses Vorgehen zulässig.

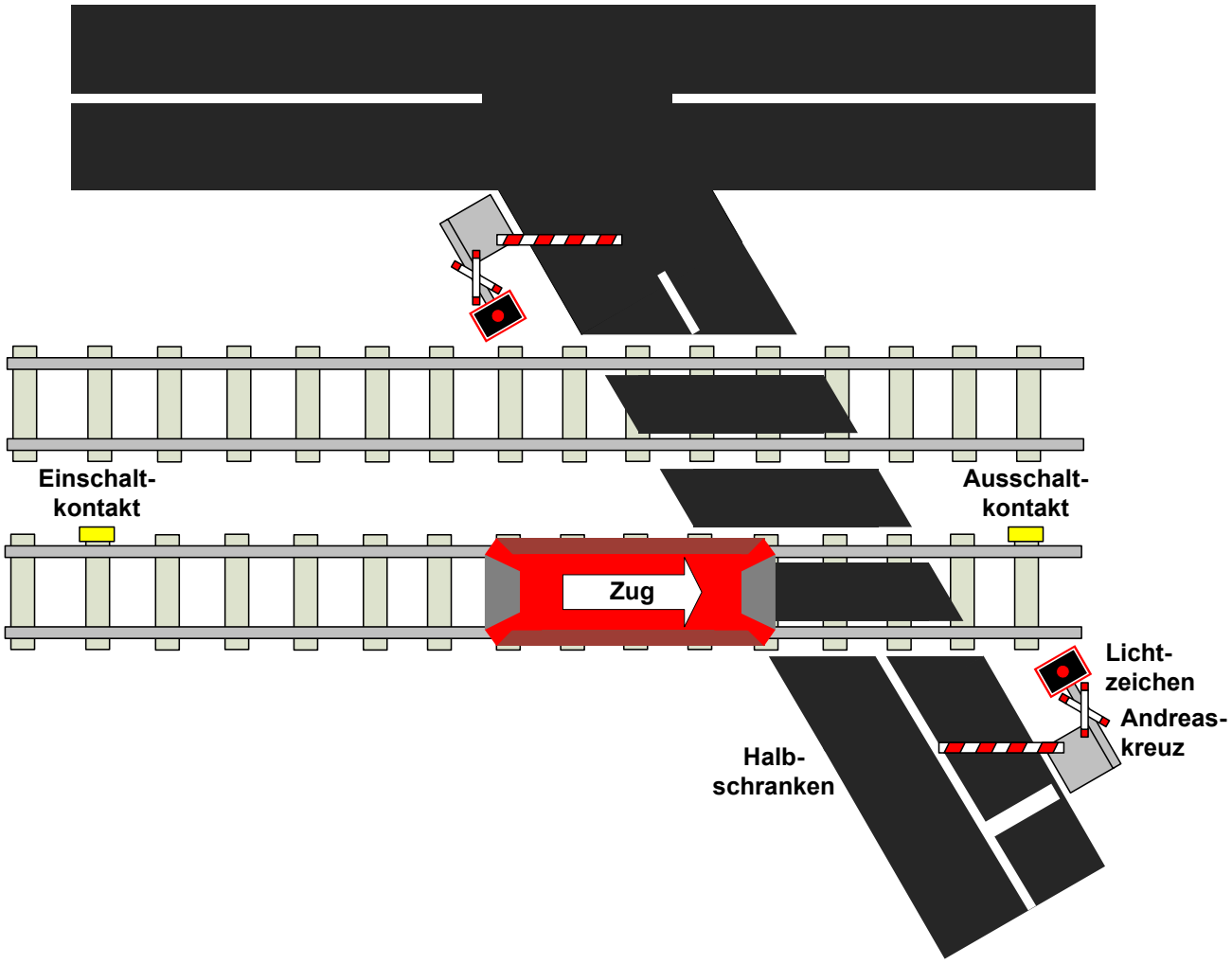

Abbildung 10.1: Bahnübergang Wupperweg

[1] Die Zeitungsartikel sind in Anhang C wiedergegeben.

Zum System Bahnübergang Wupperweg gehören (siehe auch Abbildung 10.1)

- Andreaskreuze
- rote Blinklichter
- zwei Gleise
- Einschalt- und Ausschaltkontakte seitlich der Schienen
- Halbschranken

Aus den Artikeln (siehe Anhang C) lässt sich schließen, um welchen Typ Bahnübergang es sich auf dem Wupperweg handelt. Da der Bahnübergang über Einschaltkontakte verfügt, wird er zuggesteuert eingeschaltet. Nach Tabelle 8.1 kommen damit die Typen ÜS, $ÜS_{OE}$, Hp_{OE} oder Fü in Frage. Wäre der BÜ mit einem Überwachungssignal ausgestattet (also vom Typ ÜS), dann hätte für den Beinahe-Unfall ein Defekt im Überwachungssignal vorliegen müssen, der in der Presse wahrscheinlich erwähnt worden wäre. Der BÜ wurde in den 1960ern gebaut [Sti10], daher kann er nicht vom Typ $ÜS_{OE}$ oder Hp_{OE} sein, denn diese Typen wurden erst später entwickelt. Daher kann angenommen werden, dass der Bahnübergang Wupperweg vom Typ Fü, also fernüberwacht ist. Das bedeutet, dass am BÜ kein Signal steht, dass Auskunft darüber gibt, ob der BÜ gesichert wurde. Damit ist die oben aufgeführte Liste mit Komponenten des BÜ ausreichend vollständig.

Aus Platzgründen und weil kein offizieller Untersuchungsbericht vorliegt wird an dieser Stelle keine vollständige WBA durchgeführt. Stattdessen soll zur Verdeutlichung der Zusammenhänge zwischen WBA und Sicherheitsschichten ein Ausschnitt aus dem Why-Because-Graphen genügen. Als zu untersuchendes Ereignis wird für die WBA das gleiche Ereignis wie in Kapitel 9 gewählt: „Zug befährt ungesicherten Bahnübergang“.

Ein Ausschnitt aus dem WBG für das zu untersuchende Ereignis ist in Abbildung 10.2 dargestellt. Es wurden nur die kausalen Faktoren aufgenommen, die anhand der Zeitungsartikel belegt werden können oder auf die aufgrund der Informationslage geschlossen werden kann.

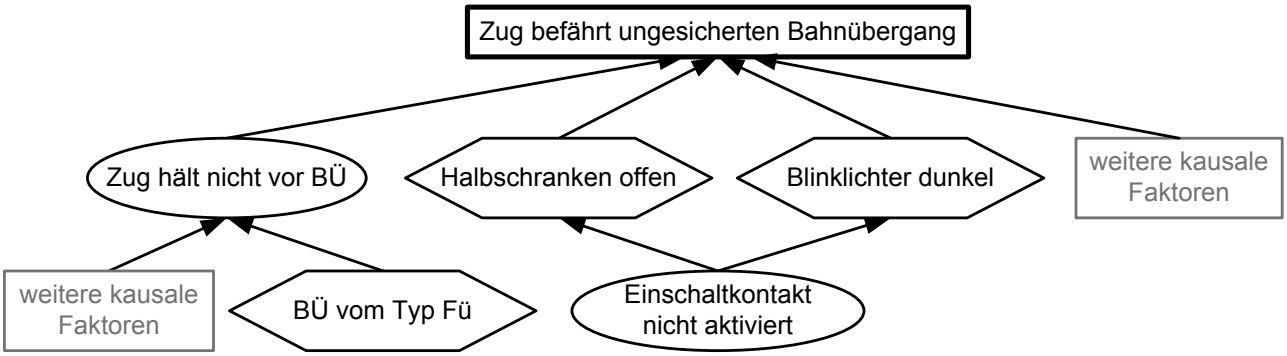

Abbildung 10.2: Why-Because-Graph des Vorfalls am Bahnübergang Wupperweg (Ausschnitt)

Laut den Aussagen eines Bahnsprechers wurde der elektrische Kontakt an den Gleisen nicht aktiviert [Taa10]. Da dieser Einschaltkontakt nicht nur das Senken der Halbschranken, sondern auch das Blinken der roten Blinklichter auslöst, kann davon ausgegangen werden, dass zum fraglichen Zeitpunkt nicht nur die Halbschranken offen, sondern auch die Blinklichter dunkel blieben. Weiterhin ist den Zeitungsartikeln zu entnehmen, dass der Triebfahrzeugführer (Tf) den Zug nicht vor dem BÜ angehalten hat. Ein kausaler Faktor hierfür ist der Typ des Bahnübergangs, der dem Tf keine Auskunft über den Status des BÜ gibt. Über weitere kausale Faktoren wie die Beschaffenheit der Strecke oder die Geschwindigkeit des Zuges, die die Möglichkeit des rechtzeitigen Erkennens der Situation durch den Tf beeinflussen, kann an dieser Stelle nur spekuliert werden.

10.2.3 Theoretischer Zusammenhang zwischen Why-Because-Analyse und Schweizer-Käse-Modell

Der prinzipielle Zusammenhang zwischen Unfallanalysen, die mit der Methode WBA durchgeführt wurden, und Sicherheitsschichten wurde bereits in [PSM07] und [SP07] dargestellt. Der WBG, der im Rahmen einer WBA erstellt wird, beschreibt den Unfallhergang in Form eines Graphen, in dem alle kausalen Faktoren für den Unfall enthalten sind. Die Grundursachen bilden zusammen einen zugleich notwendigen als auch hinreichenden Satz von kausalen Faktoren, die zum Eintreten des Unfalls geführt haben. D. h. alle diese Ursachen müssen eintreten, damit es zu dem Unfall kommen kann.

Im Schweizer-Käse-Modell (SCM) müssen alle als Käsescheiben dargestellten Sicherheitsschichten durchbrochen werden, damit es zu einem Unfall kommen kann. Der Pfeil im SCM stellt den Unfallhergang dar. Trifft er auf ein Loch in einer Sicherheitsschicht, so wird diese Sicherheitsschicht durchbrochen. Folglich bilden alle Löcher, die im SCM von einem Pfeil durchbrochen werden, einen notwendigen und hinreichenden Satz von kausalen Faktoren, die zum Eintreten des Unfalls geführt haben. Die Grundursachen des WBG entsprechen demnach Löchern in den Sicherheitsschichten entlang des Pfeils des Unfallhergangs. Dieser Zusammenhang lässt sich wie in Abbildung 10.3 graphisch darstellen. Eine Besonderheit sind kausale Faktoren, die sich keiner Sicherheitsschicht zuordnen lassen. Sie deuten auf eine fehlende Sicherheitsschicht hin, d. h. eine Sicherheitsschicht, die im System nicht vorhanden ist.

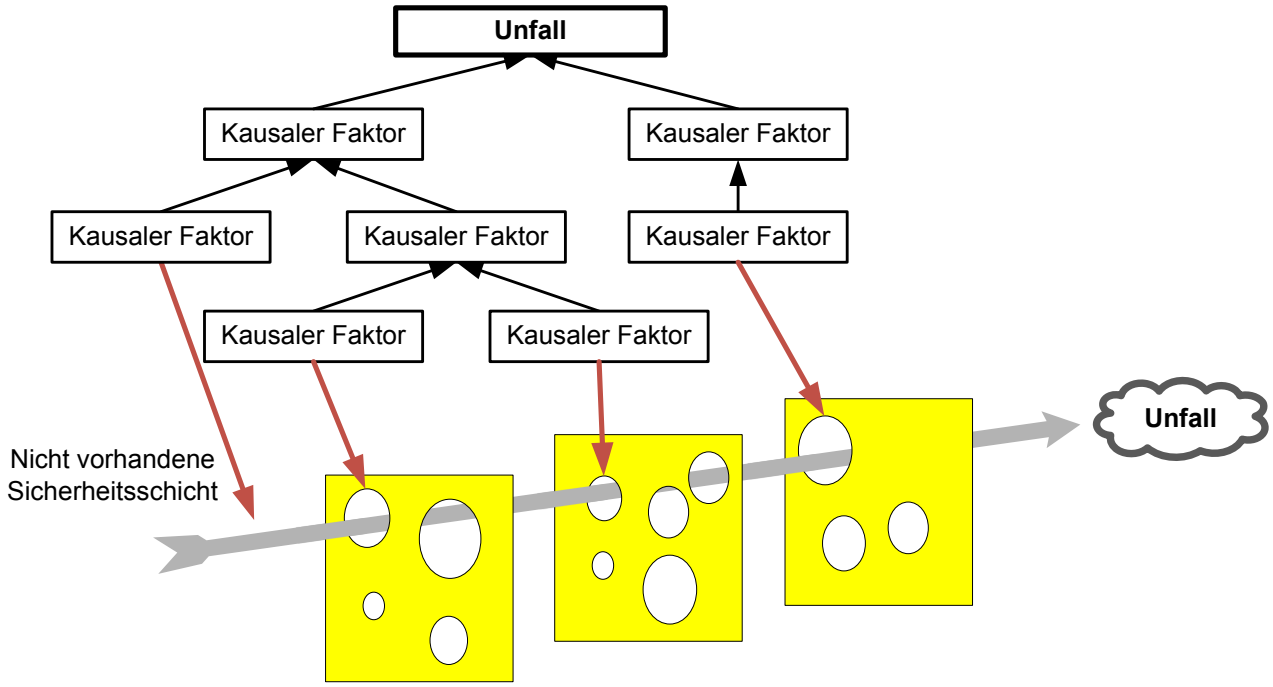

Abbildung 10.3: Zusammenhang zwischen Why-Because-Graph und Schweizer-Käse-Modell

Der Zusammenhang mit den Löchern im SCM gilt nicht nur für die Grundursachen des WBG, sondern auch für jeden anderen Satz von kausalen Faktoren, der das Eintreten des Unfalls hinreichend begründet. Die Detaillierungsebene eines WBG ist nicht vorgegeben, sondern wird vom Analysten frei nach seinen Bedürfnissen gewählt. Eine tiefere Detaillierungsebene entspricht im SCM dem Zerschneiden des Käses in eine größere Anzahl von dünneren Scheiben. Das Zusammenfassen und Aufspalten von Sicherheitsschichten ist in [SP07] näher ausgeführt.

10.2.4 Zusammenhang zwischen Why-Because-Graph und identifizierten Sicherheitsschichten

Der Bahnübergang aus Kapitel 8 entspricht nicht ganz dem Bahnübergang auf dem Wupperweg, ist ihm jedoch in vielen Punkten ähnlich. Beide Bahnübergänge verfügen über Halbschranken und über optische Warnsignale für den Straßenverkehr. Beide Bahnübergänge haben einen Einschaltkontakt. Diese Ähnlichkeit genügt, um den Zusammenhang zwischen den (Grund-)Ursachen des Beinahe-Unfalls und dem Modell der Sicherheitsschichten des Bahnübergangs aus Kapitel 9 darzustellen.
Die Sicherheitsschichten des Beispiel-Bahnübergangs wurden in Abschnitt 9.4 bestimmt. Ihr Zusammenhang mit den (Grund-)Ursachen im WBG des Beinahe-Unfalls am Bahnübergang Wupperweg ist in Abbildung 10.4 dargestellt.

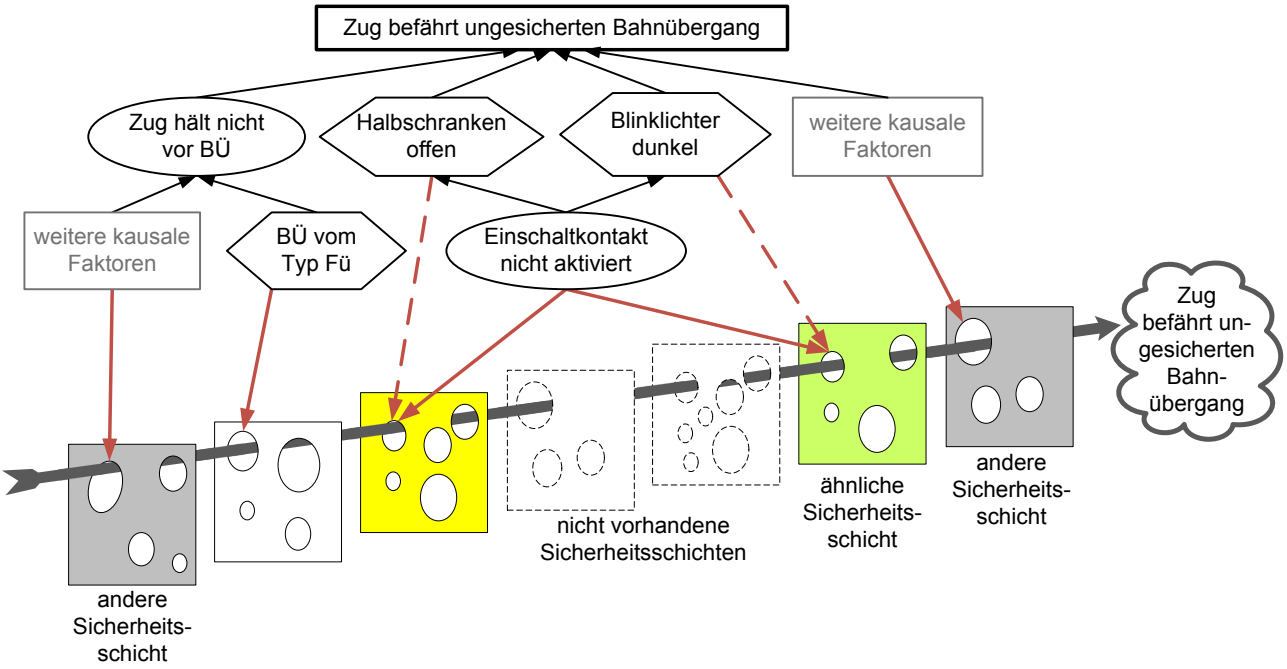

Abbildung 10.4: Zusammenhang zwischen den Sicherheitsschichten des Beispiel-Bahnübergangs und dem Why-Because-Graphen für den Beinahe-Unfall auf dem Wupperweg (Prinzipdarstellung)

Der Beispiel-Bahnübergang aus Kapitel 9 besitzt 6 Sicherheitsschichten. Eine von ihnen, die Sicherheitsschicht IV (Barriere: Halbschranken), ist auch am Bahnübergang Wupperweg vorhanden. Sie ist in Abbildung 10.4 gelb dargestellt. Die Sicherheitsschichten II und III des Beispiel-Bahnübergangs (mit den Barrieren gelbe und rote Lichtzeichen) sind am Wupperweg nicht vorhanden. Stattdessen wird dort eine ähnliche Sicherheitsschicht mit der Barriere Blinklichter verwendet (grün dargestellt). Die weiß und gestrichelt dargestellten Sicherheitsschichten in Abbildung 10.4 repräsentieren die Sicherheitsschichten I und V des Beispiels aus Kapitel 9 (Barrieren: PZB und Überwachungssignal). Sie sind am Bahnübergang Wupperweg nicht vorhanden, da es sich dort nicht um einen Bahnübergang vom Typ ÜS handelt. Stattdessen ist in Abbildung 10.4 eine Sicherheitsschicht dargestellt, die die Überwachungsart Fü repräsentiert. Daneben besitzt der Bahnübergang Wupperweg noch weitere Sicherheitsschichten (grau dargestellt), die im WBG aus Platzgründen nicht weiter detailliert wurden.

10.2.5 Fazit

Der Zusammenhang zwischen dem Ergebnis der ISES-Methode und Unfallanalysen wurde erläutert und am Beispiel der Unfallanalysemethode WBA detailliert. Die kausalen Faktoren aus dem WBG

haben eine Entsprechung in den Sicherheitsschichten: Sie beschreiben Schwächen der Sicherheitsschichten – im Schweizer-Käse-Modell entspricht das den Löchern in den Käsescheiben.
Wenn für ein System eine Analyse mit der ISES-Methode durchgeführt wird, ist zu erwarten, dass die Kenntnis über die Sicherheitsschichten des Systems die Durchführung von Unfallanalysen erleichtert. Die Sicherheitsschichten (SiS) bilden eine Gruppe von Systemelementen, die bei einer Unfallanalyse untersucht werden müssen. Durch eine vollständige Identifikation der SiS kann die Unfallanalyse nicht nur erleichtert, sondern auch strukturiert und geführt werden. Dies ist besonders hilfreich, da viele Unfallanalysen als Eingangsinformationen nur Systembeschreibungen und Unfallberichte in Textform, Interviews und eine direkte Begehung des Unfallorts verwenden. Die wesentlichen Sicherheitsmechanismen und wie diese versagt haben, müssen aus diesen Eingangsinformationen erst herausgefiltert werden. Die Kenntnis der Sicherheitsschichten eines Systems erleichtert dies deutlich. Darüber hinaus können aus Unfallanalysen resultierende Verbesserungsvorschläge direkt auf einzelne Sicherheitsschichten Bezug nehmen (Stärkung der SiS) oder selbst eine neue SiS bilden, die dann ins Modell der Sicherheitsschichten mit aufgenommen werden kann.
Das Modell der Sicherheitsschichten fügt sich in bestehende Konzepte aus dem Bereich der Unfallanalyse ein. Dies wurde anhand des Beinahe-Unfalls am Bahnübergang Wupperweg demonstriert.

11 Zusammenfassung und Ausblick

11.1 Zusammenfassung

An das Eisenbahnsystem werden nicht nur hohe Sicherheitsanforderungen gestellt, Eisenbahnen müssen die Sicherheit ihrer Systeme auch nachweisen, bevor diese Systeme in Betrieb genommen werden dürfen. Um die Sicherheit eines Eisenbahnsystems nachzuweisen, können gemäß der *gemeinsamen Sicherheitsmethode (CSM) für die Evaluierung und Bewertung von Risiken* verschiedene Strategien verfolgt werden, darunter der Vergleich mit den anerkannten Regeln der Technik und der Vergleich mit Referenzsystemen. Eine Schwierigkeit bei solchen Vergleichen besteht jedoch oft in der Unterscheidung zwischen sicherheitsrelevanten und nicht-sicherheitsrelevanten Systemelementen und Regeln. Die von Herstellern und Betreibern verwendete Dokumentation ihrer Systeme ist aus verständlichen Gründen mehr auf die Beschreibung der betrieblichen und funktionalen Aspekte ausgerichtet als auf den Nachweis der Sicherheit.
Der Begriff der *Sicherheitsschicht* bietet eine Möglichkeit der Beschreibung der sicherheitsrelevanten Teile eines Systems, die für die Sicherheitsnachweisführung von Vorteil ist. Der Inhalt dieses Begriffs wurde in der vorliegenden Arbeit nach einer ausführlichen Analyse der vorhandenen Begriffswelt neu definiert und mit klaren Prüfkriterien verbunden. Sicherheitsschichten berücksichtigen den funktionalen Ansatz der CENELEC-Normen und sind zur Verwendung in Sicherheitsnachweisen geeignet. Sie sind durch die an sie gestellten Unabhängigkeitsanforderungen so gestaltet, dass sie den Aufbau eines Portfolios aus Sicherheitsmaßnahmen im Eisenbahnsystem ermöglichen, das zukünftige Analysen und Sicherheitsnachweise erleichtern kann.
Aus verschiedenen vorhandenen Modellen und Darstellungsweisen wurde mit dem Schweizer-Käse-Modell ein geeignetes Beschreibungsmittel zur Darstellung von Sicherheitsschichten ausgewählt. Durch die einfache Darstellung mit Hilfe dieses Modells ist das Konzept der Sicherheitsschichten für Fachleute aus verschiedenen Disziplinen, wie z. B. Ingenieure, Juristen und Finanzfachkräften leicht verständlich. Dadurch wird die fachübergreifende Kommunikation erleichtert.
Um die strukturierte und effiziente Identifikation von Sicherheitsschichten im Eisenbahnsystem zu ermöglichen, wurde im Rahmen der vorliegenden Arbeit die *ISES-Methode* entwickelt. Sie bietet die Möglichkeit, die Sicherheitsschichten in existierenden Systemen, aber auch bereits im Entwurfsstadium neuer Systeme zu identifizieren. Durch sie wird die weit verbreitete „ad hoc"-Identifikation von Sicherheitsmaßnahmen abgelöst. Die ISES-Methode basiert auf einer Standard-Methode aus dem Eisenbahnbereich, der Fehlerbaumanalyse, ergänzt diese durch den Ansatz der Barriereanalyse und fügt weitere Schritte hinzu, um die verbleibenden methodischen Lücken zu schließen. Durch die Nutzung einer Checkliste bietet die ISES-Methode eine bisher im Eisenbahnbereich so noch nicht vorhandene methodische Unterstützung. Die ISES-Methode unterstützt die Sicherheitsnachweisführung nach CENELEC, indem sie die methodischen Anforderungen der DIN EN 50129 [DIN03] berücksichtigt. Ihre Ergebnisse können für den Sicherheitsnachweis gemäß DIN EN 50129 verwendet werden.
Die Beschreibung des Begriffs Sicherheitsschicht und der ISES-Methode wurde durch Regeln und Anwendungshinweise vervollständigt. Der Anwender erhält hier Hilfestellung zu Fragen des Anwendungszeitpunkts, der Modellierung und der Bewertung der Ergebnisse.
Durch die klare Definition des Begriffs Sicherheitsschicht und die ISES-Methode können verschiedene Systeme und Systementwürfe bzgl. ihrer Sicherheit miteinander verglichen werden. Auch der Abgleich von Anforderungen (z. B. aus Regelwerken oder anerkannten Regeln der Technik) und dem

tatsächlichen oder geplanten System wird durch ein Modell der Sicherheitsschichten einfach und verständlich möglich. Ebenso kann der Vergleich mit Referenzsystemen durch die Anwendung dieses Modells strukturiert und transparent erfolgen. Damit werden die beiden zuvor angesprochenen Strategien aus der CSM unterstützt. Für die dritte Strategie, eine explizite quantitative Risikoabschätzung, liefern die Ergebnisse der ISES-Methode eine Basis.
Zur Veranschaulichung der ISES-Methode wurde sie auf das Beispiel eines *Bahnübergangs* angewendet. Dabei wurden die Sicherheitsschichten des Beispiel-Bahnübergangs identifiziert, ein Modell der Sicherheitsschichten gebildet und dieses mit Hilfe des Schweizer-Käse-Modells graphisch dargestellt. Dadurch wurde die Anwendbarkeit des Konzepts der Sicherheitsschichten und der ISES-Methode für den Eisenbahnbereich belegt.
Als ein besonders relevantes Anwendungsfeld für das Modell der Sicherheitsschichten wurde die *Veränderung bestehender Systeme* identifiziert. Sicherheitsrelevante Änderungen an einem System werden als Austausch einzelner Sicherheitsschichten modelliert. Dadurch wird der Rahmen für eine Delta-Sicherheitsbetrachtung klar abgegrenzt und das Verfahren erleichtert, wodurch der Aufwand und damit die Kosten für die Sicherheitsnachweisführung reduziert werden können. Das Vorgehen für den Austausch von Sicherheitsschichten wurde beschrieben und am Beispiel der Einführung von ETCS am Beispiel-Bahnübergang verdeutlicht.
Der Begriff Sicherheitsschicht und die ISES-Methode wurden im Rahmen der vorliegenden Arbeit *validiert*. Der Nutzen und die Anwendbarkeit im Eisenbahnbereich wurden dargelegt, und es wurde gezeigt, dass sowohl der Begriff als auch die Methode alle an sie gestellten Anforderungen erfüllen.
Die vorliegende Arbeit wurde durch die Betrachtung der Verbindung zwischen Sicherheitsschichten und *Unfallanalysen* vervollständigt. Am Beispiel eines Beinahe-Unfalls an einem Bahnübergang wurde gezeigt, dass sich das Modell der Sicherheitsschichten in die bestehende Methodenwelt zur Unfalluntersuchung eingliedert. Durch die Kompatibilität mit den Ergebnissen von Unfalluntersuchungen kann das Modell der Sicherheitsschichten eines Systems derartige Analysen erleichtern. Nach Vorfällen oder Unfällen können Rückschlüsse auf das System und die Leistungsfähigkeit seiner Sicherheitsschichten gezogen werden. Durchgeführte Verbesserungsmaßnahmen lassen sich leicht im Modell der Sicherheitsschichten berücksichtigen.

11.2 Ausblick

Die in der vorliegenden Arbeit vorgestellte ISES-Methode ermöglicht eine Identifikation von Sicherheitsschichten eines Systems. Ein Teil der Methode nutzt Checklisten zur Bildung von Barriere-Funktions-Paaren und zur Identifikation von Sicherheitsmaßnahmen eines Systems. Für diese Checklisten ist im Rahmen einer beispielhaften Anwendung der Methode auf einen Bahnübergang eine Basis gelegt worden. Die erstellte Checkliste muss vervollständigt und ihr Anwendungsbereich über den eines Bahnübergangs hinaus erweitert werden. Zu diesem Zweck sollte die ISES-Methode auf weitere Systeme im Eisenbahnbereich angewendet werden. Die Checklisten sollten zudem durch eine Analyse der verschiedenen grundlegenden Regelwerke aus dem Eisenbahnbereich, z. B. der Eisenbahn-Bau- und Betriebsordnung, der Richtlinien der Deutschen Bahn AG etc. ergänzt werden. Eine vollständige Untersuchung dieser Regelwerke auf Strategien, Funktionen und Barrieren würde eine wertvolle Basis für die zukünftige Anwendung der ISES-Methode schaffen. Dabei ist auch eine Erweiterung auf den Bereich der Straße denkbar, um ein einheitliches gemeinsames Modell für den Bereich des Bahnübergangs zu schaffen.
Zur Erstellung der Checkliste im Rahmen der Anwendung der ISES-Methode auf den Beispiel-Bahnübergang wurden Ergebnisse aus den Projekten SELCAT und ROSA verwendet. Hier wird deutlich, dass in vielen Projekten immer wieder die gleiche Arbeit geleistet wird: die Identifikation von Sicherheitsmaßnahmen in Form von Barrieren und / oder Funktionen. Die Ergebnisse der Projekte sind häufig ähnlich und unterscheiden sich oft nur im Schwerpunkt der Betrachtung oder in der Formulierung. Um Synergien zu erzielen, ist es wünschenswert, diese Arbeiten zu vereinheitlichen

und dann z. B. in Form einer internationalen Norm zu veröffentlichen. Normen besitzen im Ingenieurbereich einen hohen Verbreitungsgrad – sie sind ein Standard-Arbeitsmittel. Projektberichte wie die von SELCAT oder ROSA hingegen sind weniger bekannt. Frei verfügbare Checklisten würden zu einer Standardisierung bei der Identifikation von Sicherheitsschichten führen (gleiche Detaillierungsebene und Formulierung), sodass die Ergebnisse leicht zu vergleichen wären. Hierdurch würde z. B. der Vergleich mit Referenzsystemen vereinfacht.
In einem weiteren, zukünftigen Schritt ist es notwendig, eine Methode für die qualitative und / oder quantitative Bewertung von Sicherheitsschichten bereitzustellen. Hierfür kann z. B. in Fortführung der Anwendung der Barriereanalyse ein energiebezogener Ansatz gewählt werden. Dabei kann die Schadensschwere – und damit das Risiko – nicht nur, wie bisher üblich, durch Experten geschätzt werden, sondern anhand der bei einem Unfall freiwerdenden und aufgenommenen Energie berechnet werden. Hierfür wird eine entsprechendes Formelwerk sowie eine methodische Anleitung benötigt.
Wenn die ISES-Methode durch weiterentwickelte, öffentlich zugängliche Checklisten zusammen mit einer Methode zur qualitativen oder quantitativen Bewertung der Sicherheitsschichten vervollständigt wird, kann dadurch ein standardisierter Ansatz zur Sicherheitsbetrachtung von Eisenbahnsystemen geschaffen werden. Dadurch würde ein wichtiger Beitrag geleistet, um die immer wiederkehrende Arbeit der Risikobewertung und der Erstellung von Sicherheitsnachweisen zu vereinfachen, Kosten zu senken und die Ergebnisse vergleichbar zu machen.
Neben der Anwendung der ISES-Methode im Eisenbahnbereich ist auch eine Anwendung in anderen Domänen denkbar. Die ISES-Methode ist vor allem für solche Domänen interessant, in denen es hohe Sicherheitsanforderungen gibt. In solchen Domänen wird die Sicherheit der Systeme zumeist dadurch gewährleistet, dass das Eintreten bestimmter unerwünschter Ereignisse durch den Einsatz mehrerer Maßnahmen verhindert wird. Denkbar wären hier z. B. die Prozessindustrie, der Bereich der Kernenergie und die Luftfahrt. Die Übertragbarkeit der ISES-Methode ist gegeben, da das generelle Vorgehen in den Schritten A bis D nicht domänenspezifisch ist. Die Fehlerbaumanalyse, das Konzept der Barrieren und Funktionen sowie die Kriterien für Sicherheitsschichten sind nicht auf den Eisenbahnbereich beschränkt. Lediglich die in Schritt C verwendeten Checklisten müssen für die jeweilige Domäne angepasst werden. Eine Verwendung der ISES-Methode in verschiedenen Domänen würde den interdisziplinären domänenübergreifenden fachlichen Austausch zwischen Sicherheitsexperten fördern und vereinfachen, da mit Hilfe der Modellierung von Sicherheitsmaßnahmen durch Sicherheitsschichten die Konzepte der verschiedenen Domänen auf einer geeigneten Ebene verglichen und Synergien genutzt werden können.

A Fehlerbaum

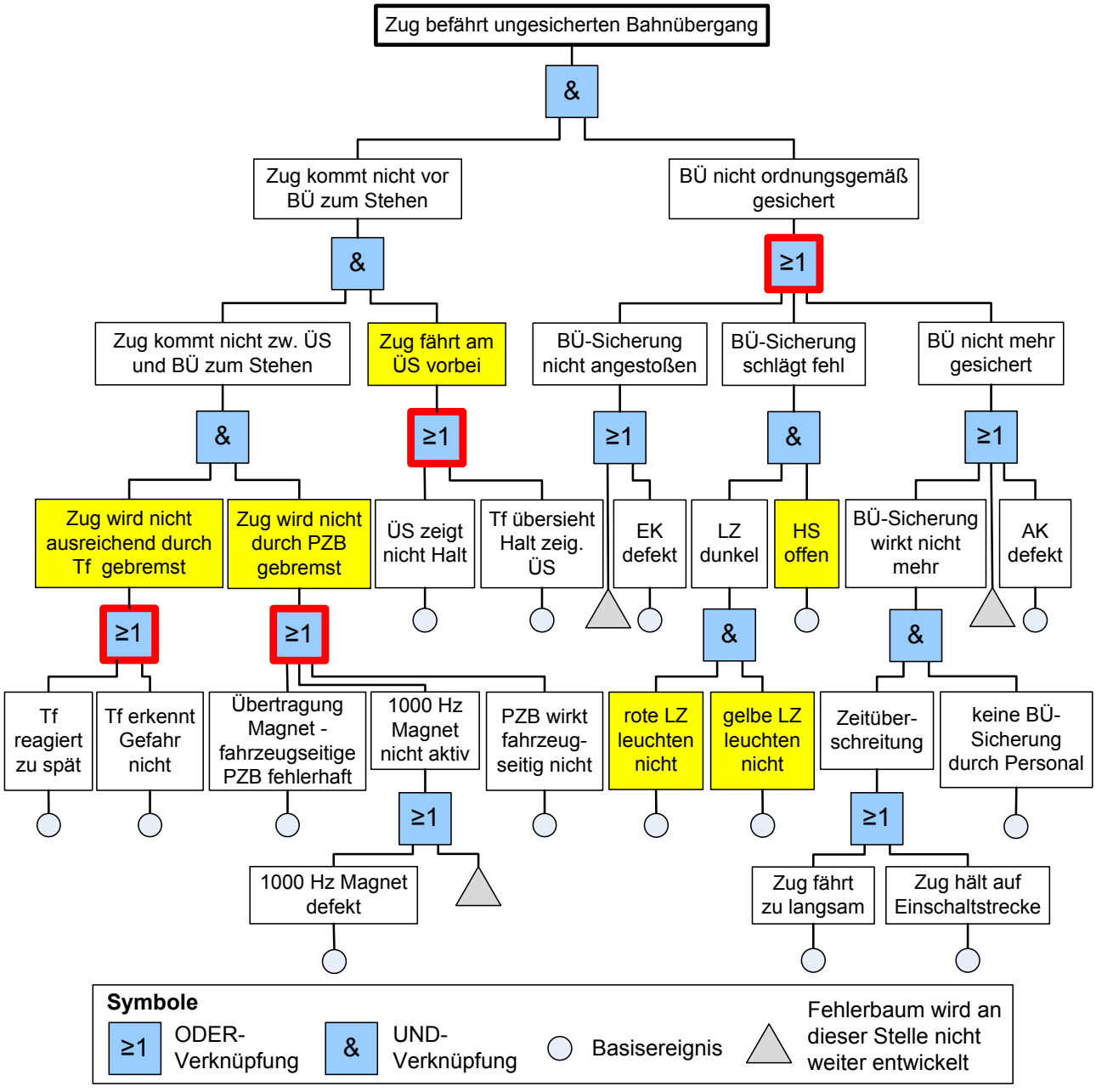

Abbildung A.1: Fehlerbaum für einen Bahnübergang mit Überwachungssignal, Ereignis „Zug befährt ungesicherten Bahnübergang“ aus [Sch10]

B Checkliste

Tabelle B.1: Strategien bei der Eisenbahn, mit Schwerpunkt auf Bahnübergängen, ergänzt um Funktionen und Barrieren aus der Analyse des Bahnübergangs aus Kapitel 9 (**fett**) (Farbbedeutung: SELCAT, ROSA, EBO)

Strategie	**Funktion**	**Subfunktion**	**Barriere / Umsetzung**
1. Reduzieren der Energiemenge	Fahrzeuggeschwindigkeit reduzieren	Geschwindigkeit für Züge beschränken	Geschwindigkeitsbeschränkung für Züge (durch Vorschrift, Schild oder Signal)
			max. 160 km/h an BÜ
		Geschwindigkeit der Züge überwachen und bei Bedarf reduzieren	Zugbeeinflussung (ATP, z. B. PZB, INDUSI, LZB)
2. Trennung von Energie und Ziel in Zeit und / oder Raum	betriebliche Regeln aufstellen	betriebliche Regeln zum Abstand Halten aufstellen	Zugleitbetrieb, StVO
		Reihenfolge festlegen	Verkehrsregel bzgl. Vorrang des Eisenbahnverkehrs, Vorfahrtsregeln (StVO)
		Betreten von Gleisanlagen verbieten	Verkehrsregeln (StVO)
	Wartepositionen festlegen		Signale und Tafeln im Bahnhof
	Arbeit so gestalten, dass das Ziel nicht so nah an die Energiequelle heran muss		Bedienung per Fernsteuerung (Rangieren)
	Verkehrswege räumlich trennen	Verkehrswege von Straßenverkehr und Schienenverkehr trennen	Bauvorschrift: Verbot von BÜ auf Strecken mit einer zugelassenen Geschwindigkeit von mehr als 160 km/h
		BÜ entfernen	Umbau
		Neubau von BÜ verhindern	Bauvorschriften, Baupläne

Tabelle B.1: Barrieremechanismen bei der Eisenbahn, mit Schwerpunkt auf Bahnübergängen (Fortsetzung)

Strategie	Funktion	Subfunktion	Barriere / Umsetzung
		Verkehrswege des Schienenverkehrs trennen	zweites Gleis
	Wege freigeben / verwehren	Straßenverkehrsteilnehmer warnen / **Straßenverkehrsteilnehmer zum Warten vor dem BÜ auffordern** / BÜ-Sicherung, Prüfung der BÜ-Sicherung	**gelbe** Lz, **rote** Lz, Blinklichter, Schranken, Halbschranken, Abschlüsse, Abschlüsse mit Sprechanlage, Posten, hörbare Zeichen, z. B. Glocke am BÜ, hörbare Signale der Eisenbahnfahrzeuge, z. B. Horn oder Pfeife des Zuges
		Züge (Tf) visuell warnen	(Licht-)Signalanlagen (Hauptsignale, Überwachungssignale)
		Züge physisch sichern / BÜ-Sicherung, Prüfung der BÜ-Sicherung	Zugbeeinflussung (ATP, z. B. PZB, INDUSI, LZB), Prüfung durch Stellwerk, Prüfung durch Personal
	bewegliche Objekte detektieren	Straßenverkehrsteilnehmer detektieren / Gefahrraumfreimeldung, BÜ beobachten / überwachen	Videokameras, Radar, technische Einrichtungen, die das Freisein des BÜ feststellen, Sicht des Schrankenwärters, **Triebfahrzeugführer**
		Züge detektieren / Aktivierung der Ankündigung des Zuges am BÜ, Gleisbelegt-Erkennung am BÜ	Achszähler, Gleisstromkreis, **Einschaltkontakt**
		Straßenverkehrsteilnehmern die Möglichkeit geben, Züge zu sehen	Übersicht
	Energiequelle außer Reichweite von Personen halten		hohe Elektrifizierung / Oberleitungen

Tabelle B.1: Barrieremechanismen bei der Eisenbahn, mit Schwerpunkt auf Bahnübergängen (Fortsetzung)

Strategie	Funktion	Subfunktion	Barriere / Umsetzung
	Ausweich- / Fluchtmöglichkeiten bieten		Halbschranken
	Aufmerksamkeit lenken	Blickrichtung der Straßenverkehrsteilnehmer in jede Richtung der Strecke lenken [FMS05]	Umlaufsperren
	Ablauf verlangsamen, um den Menschen Zeit zu geben, die Situation richtig einzuschätzen	Radfahrer zum Absteigen und Durchschieben zwingen [FMS05]	Umlaufsperren
		Geschwindigkeit für Züge beschränken	max. 160 km/h an BÜ, Geschwindigkeitsbeschränkung für Züge (durch Vorschrift, Schild oder Signal (inkl. Geschwindigkeitsüberwachung))
		Geschwindigkeit für Straßenverkehrsteilnehmer beschränken	Verkehrsschild
	Gefahrenbereich verkleinern		nur ein Gleis am BÜ
3. Isolierung durch Einfügen materieller Barrieren	Umgebung gestalten	Topographie des Geländes gestalten	Bahndamm, Zäune, Brücken, Tunnel
		Gefahrenbereich absperren, Straßenverkehrsteilnehmer physisch schützen, BÜ-Sicherung, Prüfung der BÜ-Sicherung	Halbschranken, Schranken, Abschlüsse, Abschlüsse mit Sprechanlage, Absperrungen, Tore, Rampen
		gefährliche Gegenstände vergraben / einschließen	unterirdische Verkabelung, Gehäuse von Bahnanlagen
	Fahrzeuge gestalten		stabile Hülle (Steifigkeit des Wagenkastens)

Tabelle B.1: Barrieremechanismen bei der Eisenbahn, mit Schwerpunkt auf Bahnübergängen (Fortsetzung)

Strategie	Funktion	Subfunktion	Barriere / Umsetzung
4. Verändern von Oberflächen, an denen man sich verletzen kann	abrunden von Ecken und Kanten		abgerundete Sitzkanten, Griffe
	weichmachen von Kontaktflächen		schaumstoffummantelte Stangen, gepolsterte Sitze, Gummikanten an Türen
5. Stärken des Ziels, um der Energie standzuhalten	Schutzkleidung tragen		Handschuhe
6. Schulung von Menschen zum Verhindern, dass Energie freigesetzt wird	informieren, warnen	Straßenverkehrsteilnehmer informieren	Andreaskreuz, Baken, Kennzeichnung von Privatwegen ohne öffentlichen Verkehr, Schild „Hafengebiet, Schienenfahrzeuge haben Vorrang“, Schild „Industriegebiet, Schienenfahrzeuge haben Vorrang“ an den Einfahrten zum Gebiet, Rüttelstreifen auf der Straße
		Eisenbahnpersonal informieren (ÜS ankündigen, BÜ ankündigen, . . .)	Signaltafeln, Bahnübergangstafel (Zs 9), Rautentafeln (Bü 2), Warntafel (So 15), BÜ-Ankündetafeln, BÜ-Kennzeichentafeln
		zentralen Kontrollraum informieren	Videokameras, Telefon
	unterrichten, spezielle Prozeduren / Notfallmaßnahmen schulen	Straßenverkehrsteilnehmer unterrichten	Fahrschule
		Eisenbahnpersonal unterrichten	Ausbildungsbetrieb, Berufsschule
	Regeln aufschreiben und zugänglich machen	Regeln / Prozeduren für Straßenverkehr aufschreiben und zugänglich machen	StVO
		Regeln / Prozeduren für Eisenbahnverkehr aufschreiben und zugänglich machen	Fahrdienstvorschrift

Tabelle B.1: Barrieremechanismen bei der Eisenbahn, mit Schwerpunkt auf Bahnübergängen (Fortsetzung)

Strategie	Funktion	Subfunktion	Barriere / Umsetzung
	Verhalten üben	Erlerntes auffrischen	Sicherheitstraining (Ausbildung der Tf, Vorschriften über abzuleistende Mindeststunden (Fahrpraxis), Fahrschule, Fahrsicherheitstraining)

C Bahnübergang Wupperweg

C.1 Artikel 1

Artikel aus „Kölnische Rundschau“, „rundschau-online“, im Internet verfügbar unter
http://www.rundschau-online.de/html/artikel/1288741300842.shtml,
Text kopiert am 8.2.2011:

Beinahe-Katastrophe

Zug kam: Schranke schloss sich nicht

Von Daniel Taab, 04.11.10, 17:49h, aktualisiert 04.11.10, 17:54h

Dem beherzten Tritt eines Lkw-Fahrers aufs Gaspedal ist es zu verdanken, dass es nicht zu einer Katastrophe kam: Am Bahnübergang Wupperweg schloss sich die Bahnschranke nicht. An derselben Stelle starb vor zwei Wochen ein Mietwagenfahrer.

Köln - Schon wieder ein dramatischer Vorfall am Bahnübergang Wupperweg in Höhenhaus: Am Donnerstagmittag um 13.30 Uhr fuhr die Regionalbahn 11 215 von Wuppertal nach Bonn im hohem Tempo über den beschrankten Bahnübergang - doch zum Entsetzen von Augenzeugen schlossen sich die Halbschranken nicht. Der Fahrer eines Lastwagens hatte den Zug kommen sehen. Er konnte gerade noch Gas geben und so eine Kollision verhindern. Vor zwei Wochen starb an diesem Ort ein Mietwagenfahrer, als er nach einem Unfall mit einem anderen Fahrzeug seinen Wagen von den Gleisen fahren wollte.

Der Vorfall sorgte am Nachmittag bei der Deutschen Bahn für große Aufregung. „Wir sind froh, dass nichts passiert ist. Noch können wir nicht genau sagen, warum sich die Halbschranken nicht sofort geschlossen haben“, betonte Bahnsprecher Gerd Felser. Bahn, Bundespolizei und das Eisenbahnbundesamt seien vor Ort intensiv auf der Fehlersuche. Nach ersten Erkenntnissen geht die Bahn von einer technischen Störung aus. „Der elektrische Kontakt an den Gleisen wurde offenbar nicht aktiviert“, sagte Felser. Die vorbeifahrende Bahn löse den Kontakt aus und damit das Senken der Schranken. „Das ist leider nicht passiert“, ergänzte Felser und erklärte, dass es in Nordrhein-Westfalen wohl ein einmaliger Vorfall sei. „Ich bin 13 Jahre im Job und habe so etwas hier noch nicht gehört“, so der Sprecher.

Der Lok-Führer hatte nach dem Überfahren des Übergangs die Leitstelle der Bahn informiert. Vermutlich soll der Übergang bis zur Klärung der Ursache gesperrt werden. Eine Entscheidung stand am Abend noch aus. [Taa10]

C.2 Artikel 2

Artikel aus dem „Kölner Stadt-Anzeiger“, im Internet verfügbar unter
http://www.stadtanzeiger.de/html/artikel/1288741294878.shtml,
Text und Bild kopiert am 8.2.2011:

Bahnübergang

Katastrophe nur knapp abgewendet

Von Katrin Diener, 04.11.10, 19:51h, aktualisiert 27.12.10, 20:44h

Am Bahnübergang Wupperweg ist beinahe ein Regionalzug mit einem Laster kollidiert: Als sich die Schranke öffnete, raste eine Bahn vorbei. Der Lkw konnte gerade noch bremsen. Erst vor drei Wochen gab es hier einen tödlichen Unfall.

Abbildung C.1: Bild zu Artikel 2: Die Bahnschranke am Übergang Wupperweg wird überprüft. (Bild: Stefan Worring)

Höhenhaus - Ein Regionalzug ist am Donnerstag gegen 13 Uhr beinahe mit einem Lastwagen zusammengestoßen. „Die Schranken haben sich geschlossen, aber kein Zug kam“, sagt Maria Kasten, die in Höhenhaus schräg gegenüber dem Bahnübergang am Wupperweg wohnt; „dann öffneten sich die Schranken wieder, und als ein Lkw daraufhin die Gleise überqueren wollte, raste eine Bahn vorbei. Der Lkw konnte gerade noch bremsen.“ Die 41-Jährige alarmierte die Polizei, die die Ermittlungen aufgenommen hat.

Bei dem Zug handelt es sich um den Regionalexpress 1215, der auf dem Weg von Wuppertal über Köln nach Bonn war. Die Deutsche Bahn bestätigte den Vorfall in Höhenhaus. „Es ist unerklärlich und darf nicht passieren“, sagt Sprecher Gerd Felser. „Wir sind auf der Suche nach der Ursache.“ Vorerst werden Mitarbeiter der Bahn den Bahnübergang kontrollieren und gegebenenfalls sichern. Unklar ist, ob der Vorfall im Zusammenhang mit einem Unglück steht, der sich vor drei Wochen am selben Bahnübergang ereignet hatte. Damals hatten sich die Schranken bei einem herannahenden Zug geschlossen.

Der Wagen eines 39-Jährigen war durch einen Auffahrunfall auf die Schienen geraten. Als sich einige Zeit später ein Zug näherte, soll der Mann versucht haben, das Auto noch von den Gleisen zu fahren. Der Güterzug erfasste den Wagen, der Mann starb noch an der Unfallstelle. [Die10b]

C.3 Artikel 3

Artikel aus dem „Kölner Stadt-Anzeiger“, im Internet verfügbar unter
http://www.koelner-stadt-anzeiger.com/html/artikel/1288741337353.shtml,
Text kopiert am 8.2.2011:

Deutsche Bahn

Streckenposten sichern Übergänge

Von Katrin Diener, 18.11.10, 21:10h, aktualisiert 19.11.10, 13:11h

Anfang November wäre am Bahnübergang Wupperweg beinahe eine Regionalbahn mit einem Lastwagen zusammengestoßen. Schon häufiger war die Schrankenanlage dort ausgefallen. Laut einem Sprecher ist die Bahn weiter auf Fehlersuche.

Höhenhaus - Die Suche nach der Ursache dauert an. Wie konnte es dazu kommen, dass die Regionalbahn 1215 auf dem Weg von Köln nach Wuppertal am 5. November bei nicht geschlossener Schranke über den Bahnübergang am Wupperweg fuhr? Beinahe hätte es deshalb eine Kollision mit einem Lastwagen gegeben. „Wir sind weiter auf Fehlersuche“, sagte ein Bahnsprecher. Seit dem Vorfall ist die Schrankenanlage abgeschaltet. Der Übergang wird durch zwei Streckenposten gesichert.

Die Bahn hat inzwischen auch an dem benachbarten Überweg am Mülheimer Ring die Schranke außer Betrieb genommen. „Das ist eine reine Vorsichtsmaßnahme“, sagte der Bahnsprecher. „An dieser Schranke lag kein Defekt vor. Sie haben ordnungsgemäß geschlossen. Das hängt mit Prüfungen zusammen.“ Dass das in der Nacht zum Mittwoch geschah, sei nicht ungewöhnlich. „Technisch sind die beiden Bahnübergänge baugleich. Es bestehen ähnliche Bedingungen.“ Beide Übergänge werden mit Schrankenanlagen aus den 60er Jahren gesichert. Es soll sich, so der Bahnsprecher, dabei um ein lokales Problem handeln. Weitere Bahnübergänge seien nicht betroffen.

Das Eisenbahn-Bundesamt äußert sich nur unbestimmt. „Es ist unklar, ob es einen Zusammenhang gibt oder ob an beiden Übergängen vergleichbare Probleme vorliegen“, sagte eine Sprecherin der Aufsichtsbehörde. „Im Moment gibt es keinen Anhaltspunkt für ein Systemproblem.“

Das Schließen und Öffnen der Schranken wird an beiden Bahnübergängen durch Kontaktstellen ausgelöst, die sich seitlich der Schienen befinden. Derzeit werden die Bahnübergänge von Streckenposten gesichert. Sie sperren die Trasse auf beiden Seiten mit rot-weißen Plastikband ab, bevor ein Zug kommt. Gerade an dem viel genutzten Bahnübergang Wupperweg entstehen zurzeit regelmäßig Staus. „Manchmal weiß ich gar nicht, wie ich zu meinem Haus kommen soll“, sagt Maria Kasten (41). „Und es ist ziemlich laut geworden. Weil viele Autofahrer, die hier länger als sonst stehen, anfangen zu hupen.“ Kasten wohnt direkt neben dem Übergang. „Bis die Ursache gefunden worden ist, werden die Bahnübergänge weiterhin so gesichert“, heißt es bei der Bahn. „Die Sicherheit geht vor, dafür sollten die Autofahrer Verständnis haben.“ [Die10a]

C.4 Artikel 4

Artikel aus dem „Kölner Stadt-Anzeiger“, im Internet verfügbar unter
http://www.ksta.de/jks/artikel.jsp?id=1293299399174,
Text kopiert am 28.4.2011:

Bahnübergang

Fußgänger fast von Zug erfasst

Von Tim Stinauer, 26.12.10, 23:46h, aktualisiert 17.03.11, 10:08h

Seit es am Bahnübergang Wupperweg vor einiger Zeit einen tödlichen Unfall gegeben hat, sichern Streckenposten den Übergang. Die Schranke hatte nicht zuverlässig geschlossen. Doch jetzt hat es erneut einen Zwischenfall gegeben.

Höhenhaus – *Bericht vom 26.12.2010*

Die Anwohner des Bahnübergangs am Wupperweg in Höhenhaus hatten alles andere als friedliche Feiertage. „Ich könnte in die Luft gehen, so sauer bin ich auf die Deutsche Bahn“, schimpfte Maria Kasten am Sonntag. Tags zuvor gegen 18.30 Uhr seien vor ihrem Haus beinahe zwei Frauen auf dem Bahnübergang von einem Güterzug überrollt worden, weil erneut die Schranken nicht geschlossen hätten und auch kein Signal oder Warnton die Fußgänger auf den nahenden Zug aufmerksam gemacht hätte. „Sie konnten im allerletzten Moment zur Seite springen“, schilderte Kasten, die sich im Anschluss um die ältere der beiden gekümmert hatte. Diese sei „völlig durch den Wind“ und „total fertig“ gewesen, schilderte Kasten. „Das war eine Sache von einer halben Sekunde, so knapp war das.“

Die defekte Schrankenanlage am Wupperweg ist ein bekanntes Problem. Anfang November konnte ein Lastwagenfahrer nur mit einer Vollbremsung einen Zusammenstoß mit einer Regionalbahn verhindern. Auch damals schlossen die Schranken nicht. Als Konsequenz schaltete die Deutsche Bahn die Anlage fürs erste ab und beauftragte eine Firma, die Tag und Nacht Streckenposten abstellt; sie sperren den Übergang seitdem mit rot-weißem Plastikband, sobald sich ein Zug nähert. „Aber am Samstagabend, als die beiden Frauen fast vom Zug überfahren wurden, waren die Streckenposten nicht da, und heute, am Sonntagmittag, auch nicht“, berichtete Kasten. Beides sei sehr ungewöhnlich, denn normalerweise seien die Sicherheitsleute 24 Stunden vor Ort. Der Grund ist unklar.

Die Bundespolizei wollte sich auf Anfrage des „Kölner Stadt-Anzeiger“ nicht zu dem Geschehen äußern. Ein Sprecher der Deutschen Bahn bat um Verständnis: „Da es sich um ein schwebendes Verfahren handelt, geben wir keine Auskunft.“ Womöglich, so der Sprecher, könne das Unternehmen am heutigen Montag „etwas mehr“ sagen.

Kastens Tochter (13) und deren zwei Freundinnen hatten den Beinahe-Unfall am Samstag mitangesehen. Der mit Autos beladene Güterzug sei weitergefahren, als wäre nichts geschehen. „Hier muss jetzt dringend etwas passieren“, forderte Maria Kasten. Die Schrankenanlage am Wupperweg wurde in den 1960er Jahren gebaut. Sicherheitshalber hatte die Bahn nach dem Vorfall mit dem Lastwagen im November auch einen baugleichen Übergang am Mülheimer Ring abgeschaltet und lässt ihn seither von Streckenposten überwachen. [Sti10]

C.5 Weitere Informationen

Zu den örtlichen Gegebenheiten gibt eine Satellitenaufnahme von Google Maps Aufschluss (http://maps.google.de/), siehe Abbildung C.2.

Abbildung C.2: Bahnübergang Wupperweg von oben, Google Maps, heruntergeladen am 15.2.2011

Abbildungsverzeichnis

1.1 Auszug aus der gemeinsamen Sicherheitsmethode (CSM) für die Evaluierung und Bewertung von Risiken; blau: die im Rahmen der vorliegenden Arbeit näher betrachteten Zweige . . . 2
1.2 Struktur der vorliegenden Arbeit . . . 5

2.1 Zustände eines technischen Systems im Verfügbarkeits-Sicherheitsdiagramm in Anlehnung an Schnieder [Sch03] . . . 10
2.2 Barriere . . . 11
2.3 Die fünf Level des Konzepts *Defence-in-Depth* . . . 13

3.1 Der Begriff Sicherheitsschicht als Klassendiagramm . . . 18
3.2 Bedeutung der Systemgrenzen von Sicherheitsschichten für die Unabhängigkeit . . . 21

4.1 Energiemodell in Anlehnung an Sklet [Skl06] . . . 30
4.2 Zwiebelschalenmodell nach Börcsök [BÖ6] . . . 32
4.3 Layer-of-Protection-Analysis-Diagramm (LOPA-Diagramm) in Anlehnung an Börcsök [BÖ6] und CCPS [Cen01] (Beispiel) . . . 33
4.4 Dominomodell nach Heinrich [HPR80] . . . 34
4.5 Schweizer-Käse-Modell nach Reason et al. [RHP06] . . . 35
4.6 Fliegendiagramm (Bow-Tie Diagram) in Anlehnung an Dianous et al. [DF06] . . . 36
4.7 Event and Barrier Function Model (EBFM) nach Kecklund et al. [KEWS96] (Beispiel) 37
4.8 AEB-Diagramm nach Svenson [Sve91] (Beispiel) . . . 38
4.9 Sicherheitsbarrierendiagramm nach Duijm [Dui09] (Beispiel) . . . 39
4.10 Barriereblockdiagramm nach Sklet et al. [SH04] (Beispiel) . . . 40

5.1 Why-Because-Graph in der Notation nach Sanders [SanoJ] . . . 47
5.2 Qualitativer Fehlerbaum . . . 52
5.3 Ereignisbaum für eine Bahnübergangsanlage aus [DIN08] . . . 53
5.4 Gegenüberstellung eines LOPA-Diagramms mit einem Ereignisbaum in Anlehnung an Dowell et al. [DH02] . . . 57

6.1 ISES-Methode (Methode zur Identifikation von Sicherheitsschichten in Eisenbahnsystemen) . . . 62
6.2 Schritt A der ISES-Methode . . . 64
6.3 Beispiel-System zur Geschwindigkeitsüberwachung . . . 65
6.4 Fehlerbaum für das Beispiel-System zur Geschwindigkeitsüberwachung . . . 66
6.5 Ausschnitt aus einem Fehlerbaum für einen Bahnübergang mit Überwachungssignal . 68
6.6 Reihenschaltung . . . 70
6.7 Schritt B der ISES-Methode . . . 71
6.8 Beispiel-Fehlerbaum mit markierten ersten ODER-Verknüpfungen . . . 72
6.9 Strategien aus dem Eisenbahnbereich und ihre Wirkung in einem Unfallverlauf . . . 76
6.10 Schritt C der ISES-Methode . . . 78
6.11 Unterschied zwischen einer Teilmenge (i) und anderen CCF (ii) . . . 83
6.12 Schritt D der ISES-Methode . . . 84

7.1 Sicherheitsschichten als Schweizer-Käse-Modell 88
7.2 Darstellung einer deaktivierbaren Sicherheitsschicht im Schweizer-Käse-Modell . . . 88
7.3 Darstellung einer „Lochstopfer"-Barriere im Schweizer-Käse-Modell 89
7.4 Logisches Parallelmodell als Zuverlässigkeitsblockdiagramm und im Schweizer-Käse-Modell 90
7.5 Logisches Serienmodell als Zuverlässigkeitsblockdiagramm und im Schweizer-Käse-Modell 90
7.6 Mehrere Gefährdungen für ein System: Darstellung als Schweizer-Käse-Modell, eine der gelben Sicherheitsschichten wird gegen zwei Gefährdungen verwendet 91
7.7 Vorgehen zum Austausch von Sicherheitsschichten 95

8.1 Bahnübergang mit Überwachungssignal 101

9.1 Fehlerbaum aus Sicht eines Herstellers für einen Bahnübergang mit Überwachungssignal 104
9.2 Identifizierte Sicherheitsschichten im Schweizer-Käse-Modell 124
9.3 Beispiel-Bahnübergang mit ETCS 125
9.4 Sicherheitsschichten des Beispiel-Bahnübergangs mit ETCS 126

10.1 Bahnübergang Wupperweg 139
10.2 Why-Because-Graph des Vorfalls am Bahnübergang Wupperweg (Ausschnitt) 140
10.3 Zusammenhang zwischen Why-Because-Graph und Schweizer-Käse-Modell 141
10.4 Zusammenhang zwischen den Sicherheitsschichten des Beispiel-Bahnübergangs und dem Why-Because-Graphen für den Beinahe-Unfall auf dem Wupperweg (Prinzipdarstellung) 142

A.1 Fehlerbaum für einen Bahnübergang mit Überwachungssignal, Ereignis „Zug befährt ungesicherten Bahnübergang" aus [Sch10] 149

C.1 Bild zu Artikel 2: Die Bahnschranke am Übergang Wupperweg wird überprüft. (Bild: Stefan Worring) 158
C.2 Bahnübergang Wupperweg von oben, Google Maps, heruntergeladen am 15.2.2011 . 161

Tabellenverzeichnis

4.1 Vergleich der verschiedenen Modelle und Darstellungsweisen sowie Auswahl des für den Zweck der vorliegenden Arbeit am besten geeigneten Modells, wie im Text erläutert 41

5.1 Auszug aus einer Checkliste für Energiequellen in Anlehnung an [Eri05] 50
5.2 Beispiel einer Checkliste für Barrieremechanismen, um gefährliche Energieflüsse zu steuern, in Anlehnung an [Eri05] 51
5.3 Vergleich vorhandener Methoden sowie Auswahl der für den Zweck der vorliegenden Arbeit am besten geeigneten Methoden, wie im Text erläutert 58

6.1 Basis-Checkliste zur Bestimmung von Barriere-Funktions-Paaren für den Bereich Eisenbahn 75
6.2 Identifizierte Barriere-Funktions-Paare für das Beispiel 80
6.3 Beispiel für eine Tabelle mit Barriere-Funktions-Paaren zur Prüfung der Kriterien für Sicherheitsschichten 82
6.4 Prüfung der Kriterien für Sicherheitsschichten für die Barriere-Funktions-Paare des Beispiels 85

7.1 Gefährdungs-Sicherheitsschichten-Matrix 92

8.1 Bahnübergangs-Typen in Deutschland sowie Auswahl eines Beispiel-Bahnübergangs . 99

9.1 Checkliste zur Bestimmung von Barriere-Funktions-Paaren für den Bereich Eisenbahn, ergänzt um SELCAT-Funktionen und ROSA-Barrieren für Bahnübergänge . . 107
9.2 Strategien, Funktionen und Barrieren der EBO für die Sicherheit an Bahnübergängen 110
9.3 Checkliste zur Bestimmung von Barriere-Funktions-Paaren für den Bereich Eisenbahn, ergänzt um Funktionen und Barrieren aus SELCAT, ROSA und der EBO für Bahnübergänge 112
9.4 B-F-Paare aus dem Fehlerbaum, ergänzt um Strategien und Subfunktionen; **fett gedruckt**: neue Punkte zur Ergänzung der Checkliste 117
9.5 Barriere-Funktions-Paare für den betrachteten BÜ, ergänzt um Strategien; **fett gedruckt**: neue Punkte zur Ergänzung der Checkliste; blau: Punkte, die nicht in Schritt B identifiziert wurden 120
9.6 Prüfung der Kriterien für Sicherheitsschichten für die Barriere-Funktions-Paare des Bahnübergangs-Beispiels 122

10.1 Erfüllung der Anforderungen an Sicherheitsschichten aus Abschnitt 3.1 130
10.2 Erfüllung der Anforderungen an die ISES-Methode aus Abschnitt 5.1 134

B.1 Strategien bei der Eisenbahn, mit Schwerpunkt auf Bahnübergängen, ergänzt um Funktionen und Barrieren aus der Analyse des Bahnübergangs aus Kapitel 9 (**fett**) (Farbbedeutung: SELCAT, ROSA, EBO) 151

Glossar

Ω nicht-leere Menge, Merkmalraum
◯ Basisereignis, Blatt eines Fehlerbaums
△ Fehlerbaumsymbol für „Fehlerbaum wird an dieser Stelle nicht weiterentwickelt“
$\mathfrak{A}$ σ-Algebra
$\vee$ logisches ODER
$\wedge$ logisches UND
$\boxed{\leq \mathbf{1}}$ ODER-Verknüpfung im Fehlerbaum
$\boxed{\&}$ UND-Verknüpfung im Fehlerbaum

anerkannte Regeln der Technik „Von der Mehrheit der Fachleute anerkannte, wissenschaftlich begründete, praktisch erprobte und ausreichend bewährte Regeln zum Lösen technischer Aufgaben“ [LSKM]

Ausfall 1. Ereignis: (engl. failure) „Beendigung der Funktionsfähigkeit einer materiellen Einheit im Rahmen der zugelassenen Beanspruchung“ [DIN90b, 2.2.4]. 2. Zustand: (engl. fault) „Abnormaler Zustand, der zu einem Fehler oder einer Fehlfunktion / Ausfall in einem System führen kann“ [DIN03, 3.1.18]

Ausfallrate „Wahrscheinlichkeit bezogen auf δt, dass die Betrachtungseinheit im Intervall $(t, t + \delta t)$ ausfallen wird, unter der Bedingung, dass sie zur Zeit $t = 0$ eingeschaltet wurde und im Intervall $(0, t)$ nicht ausgefallen ist“ [Bir85]. Einheit: 1 / Zeiteinheit, meist pro Stunde

Bake Straßenverkehrszeichen, das einen Bahnübergang ankündigt. Weißes Schild mit 1 bis 3 roten, schrägen Streifen

Barriere Kurzform für Sicherheitsbarriere

Barrierefunktion Kurzform für Sicherheitsbarrierefunktion

Baum Zusammenhängender Graph ohne Kreise

Begriffssystem „Begriffssystem: Geordnete Menge von Begriffen, die aufgrund ihrer Begriffsbeziehungen verbunden sind“ [Dre09]

Blatt Ein Blatt eines Baums ist ein Knoten mit genau einer Kante. Wird der Baum mit der Wurzel oben dargestellt, so sind die Blätter am unteren Ende des Baums zu finden.

CENELEC-Normen Die drei von CENELEC herausgegebenen Normen EN 50126-1, EN 50128 und EN 50129 bzw. ihre jeweiligen übersetzten nationalen Fassungen, z. B. DIN EN 50126-1 [DIN00], DIN EN 50128 [DIN12] und DIN EN 50129 [DIN03].

deduktiv Eine Methode ist deduktiv, wenn sie ausgehend von einem unerwünschten Ereignis mögliche Ursachen für dieses Ereignis betrachtet. Deduktive Methoden werden auch als Top-down-Methoden bezeichnet. Sie dienen in der Regel der Ursachenanalyse.

Energiepfad Pfad des Energieflusses von der Quelle bis zum Ziel [Eri05]

Ereignis „Übergang von einem in einen anderen Zustand“ [DIN90b]

Ereignisbaum Graphische Darstellung der verschiedenen möglichen Folgen eines Ereignisses in Form eines Baums. Ein Ereignisbaum ist ein gerichteter Baum mit dem Ereignis als Wurzel, einer Fallunterscheidung an jedem Knoten und den Endfolgen als Blättern. Ein Ereignisbaum wird in der Regel von links nach rechts gezeichnet, mit der Wurzel links. Aufgrund dieser Übereinkunft der Lesart wird bei den gerichteten Kanten auf die Darstellung als Pfeil verzichtet.

Eurobalise Eine Eurobalise (kurz: Balise) ist ein in der Gleismitte befestigter passiver Transponder, der Telegramme an darüberfahrende Züge sendet. Die Eurobalise ist ein streckenseitiges Element von ETCS.

Fehler (engl. failure) „Abweichung vom spezifizierten Verhalten des Systems“ [DIN03, 3.1.17]. Ein Fehler ist die Folge einer Fehlerursache oder eines Fehlzustandes im System [DIN03, 3.1.17]

Fehlerbaum Graphische Darstellung der logischen Zusammenhänge, die zu einem vorgegebenen unerwünschten Ereignis führen, in Form eines Baums. Ein Fehlerbaum ist durch die logischen Abhängigkeiten ein gerichteter Baum mit dem unerwünschten Ereignis als Wurzel. Ein Fehlerbaum wird in der Regel von oben nach unten gezeichnet, mit der Wurzel oben. Aufgrund dieser Übereinkunft der Lesart wird bei den gerichteten Kanten auf die Darstellung als Pfeil verzichtet.

Fehlfunktion (engl. failure) „Abweichung vom spezifizierten Verhalten des Systems“ [DIN03, 3.1.17]. Eine Fehlfunktion ist die Folge einer Fehlerursache oder eines Fehlzustandes im System [DIN03, 3.1.17].

Fehlzustand (engl. error) „Abweichung vom beabsichtigten Entwurf, die zu unerwünschtem Systemverhalten oder Ausfall führen kann“ [DIN03, 3.1.15]. Ein Fehlzustand ist latent, wenn er noch nicht als solcher erkannt worden ist [Lap92].

Funktion „Art von Aktion oder Tätigkeit, durch die ein Produkt seinen beabsichtigten Zweck erfüllt“ [DIN03, 3.1.20]. Die Beschreibung von Funktionen sollte immer ein Verb und ein Nomen enthalten.

Gefahr „Eine physikalische Situation, die potentiell einen Schaden für den Menschen beinhaltet“ [DIN00, 3.17]. Oft Synonym für Gefährdung

Gefährdung „Bedingung, die zu einem Unfall führen kann“ [DIN03, 3.1.21]. Oft Synonym für Gefahr

Gefährdungsanalyse „Prozess der Identifikation von Gefährdungen und der Analyse ihrer Ursache sowie der Ableitung von Anforderungen, um die Wahrscheinlichkeit und die Folgen von Gefährdungen auf ein akzeptables Maß zu begrenzen“ [DIN03, 3.1.22]

Graph Ein Graph besteht aus einer Menge von Knoten V, einer Menge von Kanten E und einer Abbildung, von der Menge der Kanten E in die Menge aller ungeordneten Paare von V. Eine Kante eines Graphen verbindet stets zwei Knoten, entweder zwei verschiedene Knoten, oder einen Knoten mit sich selbst (Schlinge). Graphen können ungerichtet oder gerichtet sein. Bei einem gerichteten Graphen besitzen die Kanten eine Richtung. Sie werden dann meist als Pfeile dargestellt.

Grundursache (engl. root cause) Eine Ursache für einen Unfall oder Vorfall, die ihrerseits nicht auf weitere Ursachen hin untersucht werden soll.

induktiv Eine Methode ist induktiv, wenn sie ausgehend von einem auslösenden, unerwünschten Ereignis mögliche Folgen oder Ereignisabläufe betrachtet [MP03]. Induktive Methoden werden auch als Bottom-up-Methoden bezeichnet. Sie dienen in der Regel der Folgenanalyse.

menschliches Versagen „menschliche Handlung, die zu einem ungewollten Verhalten des Systems oder zu einer Fehlfunktion führen kann“ [DIN03, 3.1.24]

Methode Ein nach Gegenstand und Ziel planmäßiges (methodisches) Verfahren, die Kunstfertigkeit einer Technik zur Lösung praktischer und theoretischer Aufgaben, besonders das Charakteristikum für wissenschaftliches Vorgehen [Bro06]

Modell „vereinfachte Darstellung der Funktion eines Gegenstands oder des Ablaufs eines Sachverhalts, die eine Untersuchung oder Erforschung erleichtert oder erst möglich macht“ [KW10]

P Wahrscheinlichkeitsmaß auf $(\Omega, \mathfrak{A})$

qualitativ Eine Methode (zur Risikoabschätzung) ist qualitativ, wenn ihre Parameter auf einer diskreten Skala gewählt werden. Bei einer diskreten Skala gibt es für Parameter eine zuvor festgelegte Anzahl von Kategorien / Klassen. (Definition nach [Mil07] und [Mil08])

quantitativ Eine Methode (zur Risikoabschätzung) ist quantitativ, wenn ihre Parameter auf einer kontinuierlichen Skala gewählt werden. Der Wert des Parameters kann dabei mit beliebiger Genauigkeit frei gewählt werden. (Definition nach [Mil08])

Risiko „Kombination aus Häufigkeit oder Wahrscheinlichkeit und den Folgen eines spezifizierten gefährlichen Ereignisses“ [DIN03, 3.1.43]

Risikoanalyse „Die systematische Auswertung aller verfügbaren Informationen zur Identifizierung von Gefährdungen und Abschätzung von Risiken“ [Eur09]

Risikominderung Minderung der Häufigkeit / Wahrscheinlichkeit oder Minderung der Folgen eines spezifizierten gefährlichen Ereignisses

Schaden „physische Verletzung oder Schädigung der Gesundheit von Menschen oder Schädigung von Gütern oder der Umwelt“ [DIN11b, 3.1.1]

Schranke Schranken sperren auf beiden Seiten eines Bahnübergangs die gesamte Straßenbreite für den Straßenverkehr. Sie werden auch als Vollschranken bezeichnet.

semi-quantitativ Eine Methode (zur Risikoabschätzung) ist semi-quantitativ, wenn sie halb-quantitativ und halb-qualitativ ist. Ihre Parameter werden auf einer diskreten Skala gewählt. Dabei werden den qualitativen Skalen numerische (quantitative) Werte zugeordnet. (Definition nach [Bep08])

sicherer Zustand „Zustand, der die Sicherheit weiterhin bewahrt“ [DIN03, 3.1.44]

Sicherheit (safety) „Das Nichtvorhandensein eines unzulässigen Schadensrisikos“ [DIN00, 3.35]

Sicherheit (security) Sicherheit im Sinne des Wachschutzes, d. h. Schutz vor Sachbeschädigung (Vandalismus), terroristischen Anschlägen, unerlaubtem Betreten, Spionage, kurz: Schutz gegen Schaden, der durch absichtliches menschliches Handeln entsteht. Der Begriff *security* beschreibt auch die Sicherheit im militärischen Sinne.

Sicherheitsanalyse Systematische Vorgehensweise zur Analyse von Systemen, um Gefährdungen und Sicherheitseigenschaften zu identifizieren und zu bewerten [HR01]

Sicherheitsbarriere physisches und / oder nicht-physisches Mittel, das geplant wurde, um unerwünschte Ereignisse oder Unfälle zu vermeiden, zu beherrschen oder abzumildern [Skl06]

Sicherheitsbarrierefunktion Funktion, die geplant wurde, um unerwünschte Ereignisse oder Unfälle zu vermeiden, zu beherrschen oder abzumildern [Skl06]

Sicherheitsfunktion technische, organisatorische oder kombinierte Funktion, die die Wahrscheinlichkeit und / oder die Folgen von Unfällen oder anderen unerwünschten Ereignissen in einem System verringern kann [HR01]

Sicherheitsintegritätslevel (SIL) „Eine von einer festgelegten Anzahl diskreter Stufen für die Spezifizierung der ausreichenden Sicherheit von Sicherheitsfunktionen, die sicherheitsrelevanten Systemen zugeordnet sind“ [DIN00, 3.38]

sicherheitskritische Funktion Funktion eines Systems, bei der eine Fehlfunktion sofort das Risiko von Verletzungen oder Gesundheitsschäden erhöhen würde [JHVR06]

Sicherheitsnachweis „Dokumentierter Nachweis, dass ein Produkt die spezifizierten Sicherheitsanforderungen erfüllt“ [DIN03]. Ein Sicherheitsnachweis gemäß DIN EN 50129 [DIN03] besteht aus sechs Teilen: Teil 1: Definition des Systems, Teil 2: Qualitätsmanagementbericht, Teil 3: Sicherheitsmanagementbericht, Teil 4: Technischer Sicherheitsbericht, Teil 5: Beziehungen zu anderen Sicherheitsnachweisen, Teil 6: Zusammenfassung.

sicherheitsrelevant „trägt Sicherheitsverantwortung“ [DIN03, 3.1.56]

System „Menge von Teilsystemen, die entsprechend einem Entwurf zusammenwirken“ [DIN03, 3.1.62]

unerwünschtes Ereignis Ein Ereignis, dessen Eintreten unerwünscht ist und daher vermieden

werden soll. Zu den unerwünschten Ereignissen zählen in der Regel Unfälle, gefährliche Vorfälle sowie Ereignisse, die das Risiko für das Auftreten der beiden genannten erhöhen.

Unfall „Ein nicht beabsichtigtes Ereignis oder eine Reihe von Ereignissen mit der Folge von Toten, von Verletzten, des Verlustes eines Systems oder von Umweltschäden“ [DIN03, 3.1.1]

Validierung „Bestätigung durch Überprüfung und objektiven Nachweis, dass die besonderen Anforderungen für einen spezifischen, bestimmungsgemäßen Gebrauch erfüllt wurden“ [DIN00, 3.44]

Verfügbarkeit „Die Fähigkeit eines Produkts, in einem Zustand zu sein, in dem es unter vorgegebenen Bedingungen zu einem vorgegebenen Zeitpunkt oder während einer vorgegebenen Zeitspanne eine geforderte Funktion erfüllen kann unter der Voraussetzung, dass die geforderten äußeren Hilfsmittel bereitstehen“ [DIN00, 3.4]

Verifikation „Bestätigung durch Überprüfung und objektiven Nachweis, dass die festgelegten Anforderungen erfüllt wurden.“ [DIN00, 3.45]

Vorfall Ein unerwünschtes Ereignis, dass beinahe Schäden oder Verletzungen verursacht hätte. Auch: Beinahe-Unfall. [HR01]

Wurzel Die Wurzel eines (gerichteten) Baums ist der einzige Knoten des Baums, der keinen Vorgänger hat. Von der Wurzel aus sind alle anderen Knoten des Baums erreichbar. Die Wurzel des Baums wird meist als oberster Knoten gezeichnet.

Zuverlässigkeitsblockdiagramm (engl. Reliability Block Diagram (RBD)) streng mathematisch aufgebautes Diagramm, in dem Bauteile eines Systems als Blöcke dargestellt werden. Die Blöcke werden so angeordnet, dass sie die logischen Relationen zwischen potentiellen Ausfällen der Bauteile darstellen. Vertikale Anordnung stellt parallele funktionale Wege dar (ODER), horizontale Anordnung eine Folge von Wegen (UND). [Bö6]

Abkürzungen

AEB Accident Evolution and Barrier function
AEG Allgemeines Eisenbahngesetz
ALARP so niedrig wie vernünftigerweise ausführbar (As Low As Reasonably Practicable)
ATP automatische Zugsicherung (Automatic Train Protection)

B-F-Paar Barriere-Funktions-Paar
BA Barriereanalyse
BBD Barriereblockdiagramm
BOStrab Verordnung über den Bau und Betrieb der Straßenbahnen (Straßenbahn-Bau- und Betriebsordnung)
BS British Standard
BÜ Bahnübergang

CCF Ausfälle aufgrund gemeinsamer Ursache (Common Cause Failures)
CCFA Analyse von Ausfällen aufgrund gemeinsamer Ursache (Common Cause Failure Analysis)
CCPS Center for Chemical Process Safety
CENELEC Europäisches Komitee für elektrotechnische Normung (Comité Européen de Normalisation Electrotechnique)
CSM Gemeinsame Sicherheitsmethode (Common Safety Method)

DIN Deutsches Institut für Normung

E/E/PE elektrisch / elektronisch / programmierbar elektronisch
EBA Eisenbahn-Bundesamt
EBFM Event and Barrier Function Model
EBO Eisenbahn-Bau- und Betriebsordnung
EN Europäische Norm
ERA Europäische Eisenbahnagentur (European Railway Agency)
ETA Ereignisbaumanalyse (Event Tree Analysis)
ETBA Energy Trace and Barrier Analysis
ETCS European Train Control System
EU Europäische Union
EUC Equipment Under Control

Fdl Fahrdienstleiter
FFB FunkFahrBetrieb
FMEA Fehler-Möglichkeits- und Einfluss-Analyse (Failure Modes and Effects Analysis)
FMECA Fehler-Möglichkeits-, Einfluss- und Kritikalitäts-Analyse (Failure Modes, Effects and Criticality Analysis)
FTA Fehlerbaumanalyse (Fault Tree Analysis)
Fü fernüberwacht

h Stunde
HAZOP Gefährdungs- und Funktionsfähigkeitsuntersuchungen (Hazard and Operability Studies)
Hp Hauptsignal

Hp_{OE} Hauptsignalabhängigkeit mit optimierter Einschaltung
HR Gefährdungsrate (Hazard Rate)
HRA Human Reliability Assessment
Hz Hertz

id identisch
INDUSI induktive Zugsicherung
IPL Independent Protection Layer
ISES Identifikation von Sicherheitsschichten in Eisenbahnsystemen

LC Bahnübergang (Level Crossing)
LEU Lineside Electronic Unit
Lf Langsamfahrsignal
LKW Lastkraftwagen
LOPA Schutzebenenanalyse (Layer of Protection Analysis)
Lz Lichtzeichen
LZB Linienförmige Zugbeeinflussung

M Mensch
MEM Minimale endogene Sterblichkeit (Minimum Endogenous Mortality)
MGS Mindestens Gleiche Sicherheit
MORT Management Oversight and Risk Tree

n. a. nicht anwendbar
NF Französische Norm (Norme Française)

PKW Personenkraftwagen
PRA Probabilistic Risk Assessment
PZB punktförmige Zugbeeinflussung

RAM Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit (Reliability, Availability, Maintainability)
RAMS Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit, Sicherheit (Reliability, Availability, Maintainability, Safety)
ROSA Rail Optimisation Safety Analysis

SADT Structured Analysis and Design Technique
SBD Sicherheitsbarrierendiagramm (Safety Barrier Diagram)
SCM Schweizer-Käse-Modell (Swiss Cheese Model)
SELCAT Safer European Level Crossing Appraisal and Technology
SF Sicherheitsfunktion (Safety Function)
SFA Sicherheitsfunktionsanalyse (Safety Function Analysis)
SIL Sicherheitsintegritätslevel (Safety Integrity Level)
SiNa Sicherheitsnachweis
SIRF Sicherheitsrichtlinie Fahrzeug
SiS Sicherheitsschicht
StVO Straßenverkehrs-Ordnung

Tf Triebfahrzeugführer
THR tolerierbare Gefährdungsrate (Tolerable Hazard Rate)

ÜS Überwachungssignal
$ÜS_{OE}$ Überwachungssignal mit optimierter Einschaltung
USE unabhängige Schutzebene

WBA Why-Because-Analyse
WBG Why-Because-Graph

ZBD Zuverlässigkeitsblockdiagramm
ZSM Zwiebelschalenmodell

Literaturverzeichnis

[BÖ6] Börcsök, Josef: *Funktionale Sicherheit: Grundzüge sicherheitstechnischer Systeme*. Heidelberg : Hüthig, 2006

[Bep08] Bepperling, Sonja-Lara: *Validierung eines semi-quantitativen Ansatzes zur Risikobeurteilung in der Eisenbahntechnik*. Braunschweig, TU Braunschweig, Diss., 27.6.2008

[Bir85] Birolini, Alessandro: *Qualität und Zuverlässigkeit technischer Systeme: Theorie, Praxis, Management*. Berlin : Springer, 1985

[BM08] Bialas-Motyl, Anna: *Eisenbahnunfälle in der Europäischen Union 2005-2006*. `http://www.eds-destatis.de/de/publications/select.php?th=7&k=2`. Version: 1/2008, Abruf: 23.12.2010 (Eurostat DATEN kurz gefasst)

[Bra02] Braband, Jens: Methoden zur Sicherheitsanalyse und ihre praktische Anwendung. In: *SIGNAL + DRAHT* 94 (2002), Nr. 1+2, S. 9–13

[Bra05a] Braband, Jens: *Risikoanalysen in der Eisenbahn-Automatisierung*. Hamburg : Eurailpress, 2005

[Bra05b] Braband, Jens: Ein semi-quantitativer Ansatz zur Risikoanalyse in der Eisenbahnautomatisierungstechnik. In: *SIGNAL + DRAHT* 97 (2005), Nr. 10, S. 6–14

[Bro06] *Brockhaus-Enzyklopädie: Bd. 18., MATH - MOSB*. 21. Aufl. Leipzig, Mannheim : Brockhaus, 2006

[Bun09] Bundesministerium für Verkehr, Bau und Stadtentwicklung: *Allgemeines Eisenbahngesetz (AEG)*. 29.7.2009

[Bun10] Bundesministerium für Verkehr, Bau und Stadtentwicklung: *Straßenverkehrs-Ordnung (StVO)*. 1.12.2010

[Bun12] Bundesministerium für Verkehr, Bau und Stadtentwicklung: *Eisenbahn-Bau- und Betriebsordnung (EBO)*. 25.7.2012

[Cen93] Center for Chemical Process Safety (CCPS): *Guidelines for safe automation of chemical processes*. New York, N.Y. : American Institute of Chemical Engineers and Center for Chemical Process Safety of the American Institute of Chemical Engineers, 1993

[CEN99] Norm EN 50126 1999. *Railway Applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS)*

[Cen01] Center for Chemical Process Safety (CCPS): *Layer of Protection Analysis: Simplified Process Risk Assessment*. Wiley, 2001

[CEN07] CENELEC: *CLC/TR 50126-2: 2007: Bahnanwendungen – Spezifikation und Nachweis der Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit und Sicherheit (RAMS) – Teil 2: Leitfaden zur Anwendung der EN 50126-1 für Sicherheit*. 2007

[CEN08] CENELEC: *CLC/TR 50126-3: 2008: Bahnanwendungen – Spezifikation und Nachweis der Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit, Sicherheit (RAMS) – Teil 3: Leitfaden zur Anwendung der EN 50126-1 für Bahnfahrzeuge RAM*. 2008

[DBA09] *Schlussbericht des Projektes ROSA (Rail Optimisation Safety Analysis)*. Berlin, 2009

[Deu06] DEUTSCHE BAHN AG: *Richtlinie 408 – Züge fahren und Rangieren: Modulgruppen 408.01 - 408.09*. 30.6.2006

[Deu08] DEUTSCHE BAHN AG: *Richtlinie 301 – Signalbuch: Signalordnung, Bahnbetrieb international*. 14.12.2008

[DF06] DIANOUS, Valérie de ; FIÉVEZ, Cécile: ARAMIS project: A more explicit demonstration of risk control through the use of bow-tie diagrams and the evaluation of safety barrier performance. In: *Journal of Hazardous Materials* 130 (2006), Nr. 3, S. 220–233

[DH02] DOWELL, Arthur M. ; HENDERSHOT, Dennis C.: Simplified Risk Analysis – Layer of Protection Analysis (LOPA): Paper 281a. In: *AIChE 2002 National Meeting*, 2002

[Die10a] DIENER, Katrin: Streckenposten sichern Übergänge. In: *Kölner Stadt-Anzeiger* (19.11.2010). `http://www.koelner-stadt-anzeiger.com/html/artikel/1288741337353.shtml`, Abruf: 8.2.2011

[Die10b] DIENER, Katrin: Katastrophe nur knapp abgewendet. In: *Kölner Stadt-Anzeiger* (4.11.2010). `http://www.stadtanzeiger.de/html/artikel/1288741294878.shtml`, Abruf: 8.2.2011

[DIN81] Norm DIN 25424-1 September 1981. *Fehlerbaumanalyse – Methode und Bildzeichen*

[DIN90a] Norm DIN 25424-2 April 1990. *Fehlerbaumanalyse – Handrechenverfahren zur Auswertung eines Fehlerbaums*

[DIN90b] Norm DIN 40041 Dezember 1990. *Zuverlässigkeit – Begriffe*

[DIN94] Norm DIN EN 61078 Oktober 1994. *Techniken für die Analyse der Zuverlässigkeit – Verfahren mit dem Zuverlässigkeitsblockdiagramm*

[DIN00] Norm DIN EN 50126-1 März 2000. *Bahnanwendungen – Spezifikation und Nachweis der Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit und Sicherheit (RAMS) – Teil 1: Grundlegende Anforderungen und genereller Prozess*

[DIN03] Norm DIN EN 50129 Dezember 2003. *Bahnanwendungen – Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme – Sicherheitsrelevante elektronische Systeme für Signaltechnik*

[DIN05a] Norm DIN EN 61511-1 Mai 2005. *Funktionale Sicherheit – Sicherheitstechnische Systeme für die Prozessindustrie – Teil 1: Allgemeines, Begriffe, Anforderungen an Systeme, Software und Hardware (IEC 61511-1:2003 + Corrigendum 2004)*

[DIN05b] Norm DIN EN 61511-3 Mai 2005. *Funktionale Sicherheit – Sicherheitstechnische Systeme für die Prozessindustrie – Teil 3: Anleitung für die Bestimmung der erforderlichen Sicherheits-Integritätslevel (IEC 61511-3:2003 + Corrigendum 2004)*

[DIN06] Norm DIN EN 50126 Berichtigung 1 September 2006. *Bahnanwendungen – Spezifikation und Nachweis der Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit und Sicherheit (RAMS), Berichtigungen zu DIN EN 50126*

[DIN07] Norm DIN EN 61025 August 2007. *Fehlzustandsbaumanalyse*

[DIN08] Normentwurf E DIN IEC 62502 August 2008. *Verfahren zur Analyse der Zuverlässigkeit – Ereignisbaumanalyse*

[DIN09] Normentwurf E DIN EN 15380-4 Juli 2009. *Bahnanwendungen – Kennzeichnungssystematik für Schienenfahrzeuge – Teil 4: Funktionsgruppen*

[DIN11a] Norm DIN EN 61508-1 Februar 2011. *Funktionale Sicherheit sicherheitsbezogener elektrischer / elektronischer / programmierbarer elektronischer Systeme – Teil 1: Allgemeine Anforderungen*

[DIN11b] Norm DIN EN 61508-4 Februar 2011. *Funktionale Sicherheit sicherheitsbezogener elektrischer / elektronischer / programmierbarer elektronischer Systeme – Teil 4: Begriffe und Abkürzungen*

[DIN11c] Norm DIN EN 61508-7 Februar 2011. *Funktionale Sicherheit sicherheitsbezogener elektrischer / elektronischer / programmierbarer elektronischer Systeme – Teil 7: Überblick über Verfahren und Maßnahmen*

[DIN11d] Norm DIN EN 62502 Juni 2011. *Verfahren zur Analyse der Zuverlässigkeit – Ereignisbaumanalyse (ETA)*

[DIN12] Norm DIN EN 50128 März 2012. *Bahnanwendungen – Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme – Software für Eisenbahnsteuerungs- und Überwachungssysteme*

[DM07] Drewes, Jörn ; May, Jörg: Entwicklung strukturierter Gefahrenlisten am Beispielsystem „Stellwerk“. In: *SIGNAL + DRAHT* 99 (2007), Nr. 1+2, S. 17–21

[Dre09] Drewes, Jörn: *Verkehrssicherheit im systemischen Kontext*. Braunschweig, TU Braunschweig, Diss., 2009

[Dui09] Duijm, Nijs J.: Safety-barrier diagrams as a safety management tool. In: *Reliability Engineering and System Safety* 94 (2009), S. 332–341

[EBVVD12] Eisenbahn-Bundesamt ; VDB ; VDV ; DB AG: *Sicherheitsrichtlinie Fahrzeug (SIRF)*. 1.6.2012

[ERA12] ERA, UNISIG, EEIG ERTMS USERS GROUP: *System Requirements Specification: Subset-026, 3.3.0: ERTMS/ETCS*. `http://www.era.europa.eu/Document-Register/Documents/Index004%20-%20SUBSET-026.zip`. Version: 7.3.2012, Abruf: 27.10.2012

[Eri05] Ericson, Clifton A.: *Hazard analysis techniques for system safety*. Hoboken, NJ : John Wiley & Sons, Inc. and Wiley-Interscience, 2005

[Eur96] Europäischer Rat: *RICHTLINIE 96/48/EG DES RATES vom 23. Juli 1996 über die Interoperabilität des transeuropäischen Hochgeschwindigkeitsbahnsystems*. 23.7.1996

[Eur04] Europäisches Parlament und Rat: *RICHTLINIE 2004/49/EG DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 29. April 2004 über Eisenbahnsicherheit in der Gemeinschaft und zur Änderung der Richtlinie 95/18/EG des Rates über die Erteilung von Genehmigungen an Eisenbahnunternehmen und der Richtlinie 2001/14/EG über die Zuweisung von Fahrwegkapazität der Eisenbahn, die Erhebung*

von Entgelten für die Nutzung von Eisenbahninfrastruktur und die Sicherheitsbescheinigung („Richtlinie über die Eisenbahnsicherheit“). 29.4.2004

[Eur08] Europäisches Parlament und Rat: *RICHTLINIE 2008/57/EG DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 17. Juni 2008 über die Interoperabilität des Eisenbahnsystems in der Gemeinschaft*. 17.6.2008

[Eur09] Europäische Kommission: *VERORDNUNG (EG) Nr. 352/2009 DER KOMMISSION vom 24. April 2009 über die Festlegung einer gemeinsamen Sicherheitsmethode für die Evaluierung und Bewertung von Risiken gemäß Artikel 6 Absatz 3 Buchstabe a der Richtlinie 2004/49/EG des Europäischen Parlaments und des Rates*. 29.4.2009

[FKKS02] Frei, Rudolf ; Kingston, John ; Koornneef, Floor ; Schallier, Philippe: *NRI MORT User's Manual: For use with the Management Oversight and Risk Tree analytical logic diagram: Generic Edition*. Delft, Dezember 2002

[FMS05] Freystein, Hartmut ; Muncke, Martin ; Schollmeier, Peter: *Handbuch Entwerfen von Bahnanlagen: Linienführung, Oberbau, Ingenieurbauwerke, Tunnel, Personenverkehrsanlagen, Bahnübergänge, Container-Terminals*. Hamburg : Eurailpress, 2005

[GHGP09a] Günther, Heiko ; Herr, Astrid ; Geisler, Marc ; Püttner, Rüdiger: WP 1 Deliverable – Hazard Analysis and resulting Starting Point Hazards for ROSA. In: *Schlussbericht des Projektes ROSA (Rail Optimisation Safety Analysis)*. Berlin, 2009

[GHGP09b] Günther, Heiko ; Herr, Astrid ; Geisler, Marc ; Püttner, Rüdiger: WP 1 Deliverable – ROSA Cause Consequence Analysis. In: *Schlussbericht des Projektes ROSA (Rail Optimisation Safety Analysis)*. Berlin, 2009

[GHS+09] Günther, Heiko ; Herr, Astrid ; Schütte, Jörg ; Geisler, Marc ; Püttner, Rüdiger: WP 1 Deliverable – Concept and Contexts of the ROSA Model. In: *Schlussbericht des Projektes ROSA (Rail Optimisation Safety Analysis)*. Berlin, 2009

[Had95] Haddon, William: Energy damage and the 10 countermeasure strategies: Reprint, Original von 1973. In: *Injury Prevention* (1995), Nr. 1, S. 40–44

[Ham11] Hammerl, Malte: *Analyse der menschlichen Einflussfaktoren und Zuverlässigkeit im Eisenbahnverkehr*. Braunschweig, TU Braunschweig, Diss., 2011

[Hen02] Henning, Steffen: Der Bahnübergang aus der Perspektive einer zentralisierten Betriebsführung. In: *EI – Der Eisenbahningenieur* 53 (2002), Nr. 6, S. 49–53

[Hol99] Hollnagel, Erik: *Accident analysis and barrier functions: Version 1.0: part of the project TRAIN - Traffic Safety and Information*. `http://www.it.uu.se/research/project/train/papers/AccidentAnalysis.pdf`. Version: 1999, Abruf: 15.5.2011

[HPR80] Heinrich, Herbert W. ; Petersen, Dan ; Roos, Nestor: *Industrial accident prevention. A safety management approach*. New York, Hamburg : McGraw-Hill Book, 1980

[HR10] Harms-Ringdahl, Lars: Assessing safety functions – results from a case study at an industrial workplace. In: *Safety Science* 41 (2003/10), Nr. 8, S. 701–720

[HR01] Harms-Ringdahl, Lars: *Safety analysis: Principles and practice in occupational safety*. 2. ed. London : Taylor & Francis, 2001

[HR09] Harms-Ringdahl, Lars: Analysis of safety functions and barriers in accidents. In: *Safety Science* 47 (2009), Nr. 3, S. 353–363

[HWL06] Hollnagel, Erik (Hrsg.) ; Woods, David D. (Hrsg.) ; Leveson, Nancy (Hrsg.): *Resilience engineering: Concepts and precepts*. Reprinted. Aldershot : Ashgate, 2006

[Int94] International Atomic Energy Agency (IAEA): *Übereinkommen über nukleare Sicherheit (Text in deutscher Übersetzung): CNS, INFCRIC/449*. 17.6.1994

[Int96] International Nuclear Safety Advisory Group: *INSAG*. Bd. 10: *Defence in depth in nuclear safety: A report by the International Nuclear Safety Advisory Group*. Vienna : International Atomic Energy Agency, 1996

[Jan00] Jansen, Lars: Referenzfallstudie Verkehrsleittechnik: funkbasierte Bahnübergangssteuerung. In: Schnieder, Eckehard (Hrsg.): *Forms 2000 – Formale Techniken für die Eisenbahnsicherung* Bd. 441, VDI-Verl., 2000 (Fortschritt-Berichte VDI Reihe 12 Verkehrstechnik / Fahrzeugtechnik), S. 1–10

[JHVR06] Johnsen, Stig O. ; Herrera, Ivonne A. ; Vatn, Jørn ; Rosness, Ragnar: Cross border railway operations: improving safety at cultural interfaces. In: *Cognition, Technology & Work* 8 (2006), Nr. 1, S. 76–88

[KEWS96] Kecklund, Lena J. ; Edland, Anne ; Wedin, Peter ; Svenson, Ola: Safety barrier function analysis in a process industry: A nuclear power application. In: *International Journal of Industrial Ergonomics* 17 (1996), Nr. 3, S. 275–284

[Kje00] Kjellén, Urban: *Prevention of accidents through experience feedback*. London : Taylor & Francis, 2000

[KW10] Kraif, Ursula (Hrsg.) ; Wermke, Matthias (Hrsg.): *Das Fremdwörterbuch: Auf der Grundlage der neuen amtlichen Rechtschreibregeln*. 10. Aufl. Mannheim : Dudenverlag, 2010

[Lad99] Ladkin, Peter B.: *A Quick Introduction to Why-Because Analysis*. `http://www.rvs.uni-bielefeld.de/research/WBA/`. Version: 1999, Abruf: 9.5.2010

[Lap92] Laprie, Jean-Claude: *Dependability: basic concepts and terminology: In English, French, German, Italian, and Japanese*. Wien : Springer-Verlag, 1992

[Las08] Lassen, Christopher A.: *Layer of protection analysis (LOPA) for determination of safety integrity level (SIL)*, Norwegian University of Science and Technology, Diss., 19.6.2008

[Lem05] Lemke, Oliver: *WB-Analyse des S-Bahn-Unfalls von Neufahrn*. `http://www.rvs.uni-bielefeld.de/Bieleschweig/5.5/`. Version: 15.6.2005, Abruf: 7.12.2011 (Bieleschweig-Workshops)

[LKEK+08] Lazarevic, Neda ; Khoudour, Louahdi ; El Koursi, El M. ; Machy, C. ; Roberts, Clive ; Impastato, Stefano ; Baldassarra, Alessandro ; Hantak, Helmut ; Berrado, Abdelaziz ; Cherkaoui, A. ; Collart Dutileul, S. ; Hartwig, Katrin ; Pelz, Markus ; Slovak, Roman: *SELCAT D2 – Report about Examination of actual and potential Technologies for Level Crossings: SELCAT-WP2-D2-V2*. 2008

[LSKM] Lemmer, Karsten ; Schnieder, Eckehard ; Knollmann, Volker ; May, Jörg: *Vorlesung Verkehrstechnik, WS 2006/2007*. Braunschweig,

[Mas12] MASCHEK, Ulrich: *Sicherung des Schienenverkehrs: Grundlagen und Planung der Leit- und Sicherungstechnik*. Vieweg+Teubner (GWV), 2012

[MF10] MENSE, Olaf ; FELDT, Henri: Vorschlag zur Einführung von ETCS Level 1 Limited Supervision bei der DB AG. In: *SIGNAL + DRAHT* 102 (2010), Nr. 9, S. 6–13

[Mil07] MILIUS, Birgit: A New Classification for Risk Assessment Methods. In: SCHNIEDER, Eckehard (Hrsg.) ; TARNAI, Géza (Hrsg.): *FORMS/FORMAT 2007 – 6th symposium*, GZVB, 2007, S. 258–267

[Mil08] MILIUS, Birgit: Vorschlag für eine Klassifikation von Methoden zur Risikobeurteilung. In: *SIGNAL + DRAHT* 100 (2008), Nr. 6, S. 32–37

[MP03] MEYNA, Arno ; PAULI, Bernhard: *Taschenbuch der Zuverlässigkeits- und Sicherheitstechnik: Quantitative Bewertungsverfahren*. München : Carl Hanser Verlag and Hanser, 2003 (Praxisreihe Qualitätswissen)

[NHDF96] NEOGY, P. ; HANSON, A. L. ; DAVIS, P. R. ; FENSTERMACHER, T. E.: *Hazard and Barrier Analysis Guidance Document*. Department of Energy, Office of Operating Experience Analysis and Feedback, 1996

[PINoJ] PINTSCH BAMAG GMBH: *Überwachungssignal PINTSCH BAMAG P145 / P145L / SP200: PINTSCH BAMAG Produkte*. `http://www.pintschbamag.de/fileadmin/s/documents/D_01_09.pdf`. Version: o. J., Abruf: 13.3.2011

[PSM07] PELZ, Markus ; SCHWARTZ, Stefanie ; MEYER ZU HÖRSTE, Michael: Model of Safety Layers in the Railway System – MoSiS. In: UNIVERSITÄT ZILINA (Hrsg.): *EURNEX – Zel 2007* Bd. 2, EDIS Zilina, 2007, S. 85–92

[Rea04] REASON, James: *Managing the risks of organizational accidents*. Aldershot : Ashgate, 2004

[Rea08] REASON, James: *The human contribution: Unsafe acts, accidents and heroic recoveries*. Farnham : Ashgate, 2008

[RHP06] REASON, James ; HOLLNAGEL, Erik ; PARIES, Jean: Revisiting the "Swiss Cheese" Model of Accidents. In: *Eurocontrol Experimental Centre Note* 13/06 (2006), Nr. 10/2006

[RSA08] RÅDBO, Helena ; SVEDUNG, Inge ; ANDERSSON, Ragnar: Suicide prevention in railway systems: Application of a barrier approach. In: *Safety Science* 46 (2008), Nr. 5, S. 729–737

[SanoJ] SANDERS, Jan: *Why-Because Analysis*. `http://www.rvs.uni-bielefeld.de/research/WBA/wba_on_one_page.pdf`. Version: o. J., Abruf: 15.5.2011

[Sch99] SCHNIEDER, Eckehard: *Methoden der Automatisierung: Beschreibungsmittel, Modellkonzepte und Werkzeuge für Automatisierungssysteme*. Braunschweig : Vieweg, 1999 (Studium Technik)

[Sch00] SCHNIEDER, Eckehard (Hrsg.): *Forms 2000 – Formale Techniken für die Eisenbahnsicherung*. Bd. *441*. Düsseldorf : VDI-Verl., 2000 (Fortschritt-Berichte VDI Reihe 12 Verkehrstechnik / Fahrzeugtechnik)

[Sch03] SCHNIEDER, Eckehard: Verlässlichkeit von Verkehrssystemen im Verfügbarkeits-Sicherheits-Diagramm. In: *SIGNAL + DRAHT* 95 (2003), Nr. 10, S. 6–9

[Sch05] SCHWARTZ, Stefanie: *Why Because Analyse eines Tram-Unfalls*. Dresden, 29.11.2005 (The Second Bieleschweig WBA & CausalML User Group Workshop)

[Sch07] SCHNIEDER, Eckehard (Hrsg.): *Verkehrsleittechnik: Automatisierung des Straßen- und Schienenverkehrs*. Berlin, Heidelberg : Springer-Verlag Berlin Heidelberg, 2007

[Sch09] SCHNIEDER, Lars: *Formalisierte Terminologien technischer Systeme und ihrer Zuverlässigkeit*. Braunschweig, TU Braunschweig, Diss., 2009

[Sch10] SCHWARTZ, Stefanie: Identifikation von Sicherheitsbarrieren am Bahnübergang. In: *ZEVrail* 134 (2010), Nr. 01-02, S. 38–44

[SGPS10] SCHÜTTE, Jörg ; GEISLER, Marc ; PÜTTNER, Rüdiger ; SCHINDELHAUER, Astrid: ROSA – ein generisches Sicherheits- und Barrieremodell des Bahnsystems: Ergebnisse des DEUFRAKO-Projekts ROSA (Rail Optimisation Safety Analysis). In: *EI – Der Eisenbahningenieur* (2010), Nr. 8, S. 26–30

[SH04] SKLET, Snorre ; HAUGE, Stein: *Safety barriers to prevent release of hydrocarbons during production of oil and gas: SINTEF REPORT No. STF38 A04419*. 15.9.2004

[SHF09] SCHWARTZ, Stefanie ; HAMMERL, Malte ; FELDMANN, Frederike: Quantifizierung menschlicher Fehler für Risikoanalysen. In: *SIGNAL + DRAHT* 101 (2009), Nr. 6, S. 19–23

[Skl02] SKLET, Snorre: *Methods for accident investigation: Report No. ROSS (NTNU) 200208*. Trondheim (N) : Norwegian University of Science and Technology (NTNU), 2002

[Skl04] SKLET, Snorre: Comparison of some selected methods for accident investigation. In: *Journal of Hazardous Materials* 111 (2004), S. 29–37

[Skl06] SKLET, Snorre: Safety barriers: Definition, classification, and performance. In: *Journal of Loss Prevention in the Process Industries* 19 (2006), Nr. 5, S. 494–506

[SL11] SCHWARTZ, Stefanie ; LIESCHE, Jörg: *Einführung in ETCS: European Train Control System – das einheitliche europäische Zugsteuerungs- und Zugsicherungssystem: Seminarunterlagen*. Berlin, 10.5.2011

[Slo06] SLOVÁK, Roman: *Methodische Modellierung und Analyse von Sicherungssystemen des Eisenbahnverkehrs*. Braunschweig, TU Braunschweig, Diss., 2006

[SP07] SCHWARTZ, Stefanie ; PELZ, Markus: MoSiS – Modell der Sicherheits-Schichten im Eisenbahnsystem. In: *10. Bieleschweig-Workshop zum Systems Engineering: Modellierung betrieblicher Aspekte & Risikoanalyse*, 2007 (Bieleschweig-Workshops)

[SP08] SCHWARTZ, Stefanie ; PELZ, Markus: *Safety Layers at Level Crossings: Poster*. Paris, 2008 (10th World Level Crossing Symposium)

[SS10] SCHNIEDER, Eckehard ; SCHNIEDER, Lars: Präzisierung des normativen Sicherheitsbegriffs durch formalisierte Begriffsbildung. In: WINZER, Petra (Hrsg.) ; SCHNIEDER, Eckehard (Hrsg.) ; BACH, Friedrich-Wilhelm (Hrsg.): *Sicherheitsforschung – Chancen und Perspektiven (acatech DISKUTIERT)*. Springer-Verlag, 2010, S. 73–115

[Sta10] STATISTISCHES BUNDESAMT: *175 Jahre Eisenbahn: Von 475 000 zu 2,37 Milliarden Fahrgästen: Pressemitteilung Nr.447 vom 3.12.2010*. 2010

[Sti10] Stinauer, Tim: Fußgänger fast von Zug erfasst. In: *Kölner Stadt-Anzeiger* (26.12.2010). http://www.ksta.de/jks/artikel.jsp?id=1293299399174, Abruf: 28.4.2011

[Sum03] Summers, Angela E.: Introduction to Layers of Protection Analysis. In: *Journal of Hazardous Materials* 104 (2003), Nr. 1-3, S. 163–168

[Sve91] Svenson, Ola: The Accident Evolution and Barrier Function (AEB) Model Applied to Incident Analysis in the Processing Industries. In: *Risk Analysis* 11 (1991), Nr. 3, S. 499–507

[Sve01] Svenson, Ola: Accident and Incident Analysis Based on the Accident Evolution and Barrier Function (AEB) Model. In: *Cognition, Technology & Work* 3 (2001), Nr. 1, S. 42–52

[Taa10] Taab, Daniel: Zug kam: Schranke schloss sich nicht. In: *Kölnische Rundschau, rundschau-online* (4.11.10). http://www.rundschau-online.de/html/artikel/1288741300842.shtml, Abruf: 8.2.2011

[TOSW09] Tordai, Laszlo ; Olpinski, Witold ; Schäfer, Werner ; Wegele, Stefan: *SELCAT – D1 – Report about Statistics, Database Analysis and Regulations for Level Crossing*. 24.6.2009

[U.S99] U.S. Department of Energy (DOE): *Conducting Accident Investigations: DOE Workbook: REVISION 2*. http://www.hss.doe.gov/csa/csp/aip/docs/workbook/. Version: 1.5.1999, Abruf: 15.5.2011

[VGRH81] Vesely, W. E. ; Goldberg, F. F. ; Roberts, N. H. ; Haasl, D. F.: *Fault Tree Handbook: NUREG-0492*. U.S. Nuclear Regulatory Commission, 1981

[Wal02] Walz, Guido: *Lexikon der Mathematik: in sechs Bänden*. Bd. 5. Heidelberg : Spektrum Akad. Verl., 2002

[Web10] Weber, Carsten: Eine Risikobetrachtung zum Zugleitbetrieb. In: *EI – Der Eisenbahningenieur* (2010), Nr. 8, S. 18–23

Index

AEB-Diagramm, 37, 38, 55
AEB-Methode, 55
AEB-Modell, 37, 41
anerkannte Regeln der Technik, 1, 7
Anforderungen
    an ISES-Methode, *siehe* ISES-Methode
    an Sicherheitsschicht, *siehe* Sicherheitsschicht
Austausch von Sicherheitsschichten, 124

Bahnübergang
    ETCS, 125
    FÜ, 99
    Hp, 99
    P + Lf, 99
    Postensicherung, 99
    Wupperweg, 139, 140, 157–161
    Ü, 99
    Ü + P, 99
    ÜS, 99, 100
Barriere, *siehe* Sicherheitsbarriere
Barriere-Funktions-Paar, 18
Barriereanalyse, 49
Barriereblockdiagramm, 39, 41
Barrieresystem, 19, 83
Bow-Tie Diagram, *siehe* Fliegendiagramm

CCF, 21, 23, 24, 83
CENELEC-Normen, 7, 8, 10
Checkliste, 50, 51, 73–75, 105–119, 151
CSM, 1–3

Defence, 12, 13
Defence-in-Depth, 12, 25, 53
Delta-Betrachtung, 27
DIN EN 50126-1, 7
DIN EN 50128, 7
DIN EN 50129, 7
Dominomodell, 33, 41

Energiemodell, 30, 41, 49
Energy Trace and Barrier Analysis, 49
Ereignisbaum, 32, 53
Ereignisbaumanalyse, 53
ETCS, 124–128
Event and Barrier Function Model, 37, 41

Fehlerbaum, 51, 52, 67, 90
Fehlerbaumanalyse, 51, 62, 63
Fliegendiagramm, 36, 41, 42
Funktion, *siehe* Sicherheitsbarrierefunktion

Gefährdungs-Sicherheitsschichten-Matrix, 91, 92

Independent Protection Layer, *siehe* Unabhängige Schutzebene
ISES-Methode, 61–86, 103–124, 134
    Anforderungen an, 44, 134–137

LOPA, 32, 56
LOPA-Diagramm, 32, 41

Mindestens Gleiche Sicherheit, 1, 127

Parallelmodell, 90

qualitative Analyse, 54, 93
quantitative Analyse, 52, 54, 93

Reihenschaltung, 70
Risiko, 13, 14
Risikoakzeptanz, 1–3
Risikoreduktionsfaktor, 53

Schutzebene, 13, 31, 32, 53, 56
Schutzebenenanalyse, *siehe* LOPA
Schweizer-Käse-Modell, 35, 41, 42, 87, 88, 90, 91, 124
Serienmodell, 90
sicherer Zustand, 9, 13, 14
Sicherheit
    safety, 9
    security, 9
Sicherheitsbarriere, 11, 19, 24, 30
Sicherheitsbarrierefunktion, 19, 55
Sicherheitsbarrierendiagramm, 38, 41, 45
sicherheitsbezogenes System, 14
Sicherheitsfunktion, 8, 12–14, 48
Sicherheitsfunktionsanalyse, 48
sicherheitskritische Funktion, 14
Sicherheitsnachweis, 7, 92, 93, 127, 128, 130
sicherheitsrelevant, 9
Sicherheitsschicht, 3, 17–27, 80, 84, 129

Bewertung von, 93
Anforderungen an, 17–18, 129–133
SIL, 9, 56
Strategie, 51, 75, 76, 110

Unabhängige Schutzebene, 13, 24, 56
Unabhängigkeit, 19
Unabhängigkeitskriterien, 20, 82
Unfall, 8, 138, 139
Bahnübergang Wupperweg, *siehe* Bahnübergang, Wupperweg
Unfallanalyse, 44, 138

Why-Because-Analyse, 46, 139, 141, 142
Why-Because-Graph, 46, 47, 140, 142
Zusammenhang mit Schweizer-Käse-Modell, 141
Wirksamkeit, 19
Wupperweg, 139–140, 142, 157–161

Zwiebelschalenmodell, 31